Bangalore Metropolitan Transport Corporation

Tender No: BMTC/2023-24/SE0074

Date:14.06.2023.

Request for Proposal

of

SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC

June-2023

Bangalore Metropolitan Transport Corporation
Kengal Hanumanthaiah Road, Shanthinagar
Bangalore 560027

CONTENTS

SECTION 1: LETTER OF INVITATION.....6

RFP SCHEDULE.....7

SECTION 2: INFORMATION TO BIDDERS.....8

1. INTRODUCTION.....8
2. CLARIFICATION AND AMENDMENT OF RFP DOCUMENTS.....9
3. PREPARATION OF PROPOSAL.....9
   - ***A. TECHNICAL PROPOSAL***.....*9*
   - ***B. FINANCIAL PROPOSAL***.....*10*
4. SUBMISSION, RECEIPT, AND OPENING OF PROPOSALS.....10
5. PROPOSAL EVALUATION.....11
   - ***A. GENERAL***.....*11*
   - ***B. EVALUATION OF PRE-QUALIFICATION/ELIGIBILITY CRITERIA PROPOSALS*** *11*
   - ***C. OPENING AND EVALUATION OF FINANCIAL PROPOSALS; RANKING;***.....*11*
6. NEGOTIATIONS.....11
7. AWARD OF CONTRACT.....12
8. CONFIDENTIALITY.....12
9. DATA SHEET.....12

SECTION 3: PROPOSAL SUBMISSION – STANDARD FORMS.....17

1. PROPOSAL SUBMISSION FORM.....17
2. CHECKLIST.....18
3. QUALIFICATION SUBMISSION FORM.....20
4. CERTIFICATE FROM THE STATUTORY AUDITOR REGARDING TURNOVER- MSP.....22
5. CERTIFICATE FROM THE STATUTORY AUDITOR REGARDING TURNOVER- CSP.....22
6. DECLARATION.....23
7. FORMAT FOR POWER OF ATTORNEY FOR SIGNING OF PROPOSAL.....24
8. COMMENTS AND SUGGESTIONS OF BIDDER.....25
9. DESCRIPTION OF APPROACH, METHODOLOGY, WORK PLAN AND TECHNICAL SPECIFICATIONS.....25
10. FORMAT FOR CURRICULUM VITAE (CV) OF PROPOSED MANPOWER.....26
11. FORMAT FOR AFFIDAVIT CERTIFYING THAT BIDDER IS NOT BLACKLISTED.....28
12. DECLARATION ON NO BANKRUPTCY/INSOLVENCY.....28
13. DECLARATION REGARDING RESTRICTIONS ON PUBLIC PROCUREMENTS FROM BIDDERS OF COUNTRIES WHICH SHARES A LAND BORDER WITH INDIA:.....29
14. CHECKLIST FOR MANDATORY REQUIREMENTS OF PROPOSED CSP.....31

SECTION 4: FINANCIAL PROPOSAL.....35

FORM 1: CALCULATION MATRIX FOR EVALUATION OF FINANCIAL BID.....35
FORM 2: BILL OF MATERIALS FOR CLOUD SERVICES.....36
FORM 4: MANPOWER PRICE - OPERATIONS AND MAINTENANCE PHASE.....39
FORM 5: RATE DISCOVERY CHART.....39

SECTION 5: TERMS OF REFERENCE (TOR).....51

1. ABOUT BMTC.....51
2. ABOUT BMTC'S MOBILE APP PROJECT.....51
3. BACKGROUND.....52
4. SCOPE OF WORK.....53
   - ***A. PROVISIONING, SETUP OF CLOUD SERVICES, TRAINING AND KNOWLEDGE TRANSFER***.....*53*
     - **a. PROVISIONING OF CLOUD SERVICES**.....53
     - **b. TRAINING AND KNOWLEDGE TRANSFER**.....54

c. BILL OF MATERIALS FOR CLOUD SERVICES 55
B. OPERATIONS & MAINTENANCE WITH OPTIMIZATION OF CLOUD SERVICES *58*
a) RESOURCE MANAGEMENT 58
b) PATCH & CONFIGURATION MANAGEMENT 58
c) USER ADMINISTRATION 58
d) SECURITY ADMINISTRATION 59
e) BACKUP ON CLOUD 59
f) MONITORING PERFORMANCE AND SERVICE LEVELS 59
g) USAGE REPORTING AND BILLING MANAGEMENT 60
h) SUPPORT FOR THIRD PARTY AUDITS AND COMPLIANCE 60
i) INFRASTRUCTURE EVENT MANAGEMENT 61
j) MISCELLANEOUS 61
C. ACCEPTANCE AND VALIDATION OF CLOUD ENVIRONMENT *61*
a. ACCEPTANCE TEST 61
b. STABILIZATION PHASE 62
c. GO-LIVE 62
D. EXIT MANAGEMENT PLAN / TRANSITION-OUT SERVICES *62*
E. CLOUD SERVICES SPECIFICATIONS AND REQUIREMENTS *62*
a. COMPUTE 62
b. NETWORKING 64
c. STORAGE-BLOCK STORAGE 66
d. STORAGE – OBJECT STORAGE 67
e. MANAGED RELATIONAL DATABASE AS A SERVICE 68
f. NON-RELATIONAL DATABASE 69
SECURITY AND ADMINISTRATION 70
g. DEPLOYMENT AND MANAGEMENT 71
h. APPLICATION SERVICES 73
i. HYBRID INTEGRATION 73
j. OTHER TECHNICAL REQUIREMENTS 74
k. SUPPORT 75
5. ELIGIBILITY CRITERIA 77
6. SERVICE LEVEL AGREEMENT 79
6.1. MEASUREMENT AND MONITORING *79*
6.2. PERIODIC REVIEWS *80*
6.3. PENALTIES *80*
6.4. SERVICE LEVELS *81*
7. PROJECT TIMELINES AND DELIVERABLES 86
8. PAYMENT SCHEDULE AND MILESTONE 88
9. HELP DESK AND SUPPORT 89

SECTION 6: ANNEXURES 90

ANNEXURE 1: RESOURCE PROFILES FOR MSP TEAM 90
ANNEXURE 2: CHANGE CONTROL NOTE FORMAT 91

CONTRACT FOR MANAGED SERVICE PROVIDER'S SERVICES 93

I. FORM OF CONTRACT 93

II. GENERAL CONDITION OF CONTRACT (GCC) 94

1. GENERAL PROVISIONS 94
1.1. DEFINITION *94*
1.2. LAW GOVERNING THE CONTRACT *94*
1.3. LANGUAGE *95*
1.4. NOTICES *95*
1.5. LOCATION *95*
1.6. AUTHORIZED REPRESENTATIVES *95*
1.7. TAXES AND DUTIES *95*

1.8. CONDITIONS PRECEDENT.....*95*
1.8.1. PROVISIONS TO TAKE EFFECT UPON FULFILMENT OF CONDITIONS PRECEDENT.....95
1.8.2. CONDITIONS PRECEDENT OF THE MANAGED SERVICE PROVIDER.....96
1.8.3. CONDITIONS PRECEDENT OF THE CLIENT.....96
1.8.4. EXTENSION OF TIME FOR FULFILMENT OF CONDITIONS PRECEDENT.....96
1.8.5. NON-FULFILMENT OF THE SERVICE PROVIDER'S CONDITIONS PRECEDENT.96
1.9. CHANGE OF CONTROL.....*96*
1.10. REPRESENTATIONS AND WARRANTIES.....*97*
1.10.1. REPRESENTATIONS AND WARRANTIES OF THE SERVICE PROVIDER.....97
1.10.2. REPRESENTATIONS AND WARRANTIES OF THE CLIENT OR ITS NOMINATED AGENCIES.....98
2. COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT 99
2.1. EFFECTIVENESS OF CONTRACT.....*99*
2.2. COMMENCEMENT OF SERVICES.....*99*
2.3. EXPIRATION OF CONTRACT.....*99*
2.4. MODIFICATION.....*99*
2.5. FORCE MAJEURE.....*99*
2.5.1. DEFINITION OF FORCE MAJEURE.....99
2.5.2. Force Majeure events.....99
2.6. SUSPENSION.....*101*
2.7. TERMINATION.....*101*
2.7.1. CLIENT.....101
2.7.2. BY THE MANAGED SERVICE PROVIDER.....102
2.7.3. CESSATION OF RIGHTS AND OBLIGATIONS.....102
2.7.4. CESSATION OF SERVICES.....102
2.7.5. PAYMENT UPON TERMINATION.....103
3. OBLIGATIONS OF SERVICE PROVIDER.....103
3.1. GENERAL.....*103*
3.2. CONFLICT OF INTEREST.....*103*
3.2.1. MANAGED SERVICE PROVIDER NOT TO BENEFIT FROM COMMISSIONS, DISCOUNTS, ETC.,.....103
3.2.2. PROCUREMENT RULES OF FUNDING AGENCIES.....103
3.2.3. MANAGED SERVICE PROVIDER AND AFFILIATES NOT TO ENGAGE IN CERTAIN ACTIVITIES.....103
3.2.4. PROHIBITION OF CONFLICTING ACTIVITIES.....103
3.3. CONFIDENTIALITY.....*104*
3.4. INSURANCE TO BE TAKEN OUT BY THE MANAGED SERVICE PROVIDER *104*
3.5. SERVICE PROVIDER'S ACTIONS REQUIRING CLIENT'S PRIOR APPROVAL *104*
3.6. REPORTING OBLIGATIONS.....*104*
3.7. DOCUMENTS PREPARED BY THE MANAGED SERVICE PROVIDER TO BE THE PROPERTY OF THE CLIENT.....*104*
3.8. EQUIPMENT AND MATERIALS FURNISHED BY THE CLIENT.....*105*
3.9. USE OF ASSETS BY THE MANAGED SERVICE PROVIDER.....*105*
3.10. TRANSFER OF ASSETS.....*105*
3.10.1. TRANSFER OF ASSET REGISTER.....105
3.10.2. TRANSFER OF DOCUMENTATION.....106
3.10.3. TRANSFER OF SERVICE MANAGEMENT PROCESS.....106
3.10.4. TRANSFER OF KNOWLEDGE BASE.....106
3.10.5. TRANSFER OF DATA.....106
3.10.6. TRANSFER OF SUPPORT ACTIVITIES.....106
3.11. INFORMATION SECURITY.....*107*
3.11.1. COMPLIANCES AND CERTIFICATIONS.....107
3.11.2. PRIVACY AND SECURITY SAFEGUARDS.....108

3.11.3. CONFIDENTIALITY.....108
3.12. SERVICE LEVEL AGREEMENT.....*109*
4. MANAGED SERVICE PROVIDER PERSONNEL.....109
4.1. DESCRIPTION OF PERSONNEL.....*109*
5. REMOVAL AND/OR REPLACEMENT OF PERSONNEL.....109
6. OBLIGATION OF CLIENT.....110
6.1. ASSISTANCE AND EXEMPTIONS.....*110*
6.2. SERVICES AND FACILITIES.....*110*
7. PAYMENT TO SERVICE PROVIDER.....110
7.1. PAYMENT.....*110*
7.2. CONTRACT PRICE.....*110*
7.3. PAYMENT FOR ADDITIONAL SERVICES.....*110*
7.4. TERMS AND CONDITIONS OF PAYMENT.....*110*
7.5. LIQUIDATED DAMAGES.....*111*
8. SETTLEMENT OF DISPUTE.....111
8.1. Scope of Disputes.....*111*
8.2. AMICABLE SETTLEMENT.....*111*
8.3. DISPUTE SETTLEMENT.....*112*
8.4. GOVERNING LAW AND JURISDICTION.....*112*
9. PERFORMANCE SECURITY.....112
10. INDEMNIFICATION & LIMITATION OF LIABILITY.....112
11. RISK PURCHASE.....114
12. FORMAT FOR NON-DISCLOSURE AGREEMENT (NDA).....114

SPECIAL CONDITION OF CONTRACT (S.C.C.).....119

APPENDICES.....119

SECTION 1: LETTER OF INVITATION

Bangalore Metropolitan Transport Corporation
Kengal Hanumanthaiah Road, Shanthinagar
Bangalore 560027

Tender No: BMTC/2023-24/SE0074
Date:14.06.2023

1. BMTC invites bids for **SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR PROVISION OF CLOUD SERVICES TO BMTC.**

2. The objective and detailed scope of service is mentioned in Terms of Reference **(Section 3).**

3. The **Managed Service Provider** will be selected **under Lowest Cost Selection (LCS)** and procedures described in this RFP.

4. The RFP includes the following documents:
   a. Section 1 - Letter of Invitation
   b. Section 2 - Information to Bidders
   c. Section 3 - Proposal submission - Standard Forms
   d. Section 4 - Financial Proposal
   e. Section 5 - Terms of Reference
   f. Section 6 - Annexures

Yours sincerely,
Controller of Stores & Purchases
Bangalore Metropolitan Transport Corporation
Central office, Bangalore

RFP Schedule

Tender Reference No.	Tender No: BMTC/2023-24/SE0074 Date:14.06.2023
Tender Inviting Authority	Controller of Stores and Purchases.
Website for accessing tender	https://kppp.karnataka.gov.in
The contact Person	Chief System Manager
Address to send Pre-bid queries	Controller of Stores and Purchases, BMTC Central Office, Kengal Hanumanthaiah Road, Shanthinagar, Bangalore 560027, Email. cosp@mybmtc.com , csm@mybmtc.com
Last Date to send pre-bid queries	22.06.2023 @ 17:30 Hrs.
Date of Pre-bid meeting	23.06.2023 @ 11:30 Hrs.
Place for Pre-bid meeting	4th floor, Mini meeting Hall, BMTC Central Office, Kengal Hanumanthaiah Road, Shanthinagar, Bangalore 560027
EMD	Rs.1,00,000.00(Rupees one lakh)
Nature of bid process	**Two cover system –** Pre-qualification and commercial proposals
Proposal Evaluation Process	Lowest Cost Selection (LCS)
Tender Processing Fee	Rs.500/- to be paid through e-payment mode only
Bid Submission End Date and Time	18.07.2023 @ 14:30 Hrs.
Pre-Qualification opening date and time	20.07.2023@14.30 Hrs
Financial Bid	21.07.2023@14.30 Hrs.(Tentative)
Bid Validity	90 Days from the bid submission end date

SECTION 2: INFORMATION TO BIDDERS

1. INTRODUCTION

1.1. The Client named in the "Data Sheet" will select a firm among those listed in the Letter of Invitation, in accordance with the method of selection indicated in the Data Sheet.

1.2. The Bidders are invited to submit a Technical Proposal and a Financial Proposal, as specified in the Data Sheet (the Proposal) for services required for the Assignment named in the Data Sheet. The Proposal will be the basis for contract negotiations and ultimately for a signed contract with the selected Bidder.

1.3. The Bidder must familiarize themselves with site conditions and take them into account in preparing their Proposals. To obtain first-hand information on the assignment and on the local conditions, Bidders are encouraged to visit to the Client before submitting the Proposal, and to attend a pre-proposal conference if one is specified in the Data Sheet. Attending the pre-proposal conference is optional. The Bidder's representative should contact the officials named in the Data Sheet to arrange for their visit or to obtain additional information on the pre-proposal conference. Bidders should ensure that these officials are advised of the visit in adequate time to allow them to make appropriate arrangements.

1.4. Please note that (i) the costs of preparing the proposal and of negotiating the contract, including a visit to the Client, are not reimbursable as a direct cost of the Assignment; and (ii) the Client is not bound to accept any of the Proposals submitted.

1.5. BMTC expects Bidders to provide professional, objective, and impartial advice and always hold the Client's interest's paramount, without any consideration for future work, and strictly avoid conflicts with other assignments or their own corporate interests. Bidder shall not be hired for any assignment that would conflict with their prior or current obligations to other Clients, or that may place them in a position of not being able to carry out the assignment in the best interest of the Client.

1.5.1. Without limitation on the generality of this rule, Bidders shall not be hired under the circumstances set forth below:

1.5.1.1. A firm which has been engaged by the Client to provide goods or works for a project, and any of their affiliates, shall be disqualified from providing consulting services for the same project. Conversely, firms hired to provide consulting services for the preparation or implementation of a project, and any of their affiliates, shall be disqualified from subsequently providing goods or works or services related to the initial assignment (other than a continuation of the firm's earlier consulting services) for the same project.

1.5.1.2. Bidders or any of their affiliates shall not be hired for any assignment which, by its nature, may conflict with another assignment of the Bidders of the Department.

1.5.2. Bidders may be hired for downstream work, when continuity is essential, in which case this possibility shall be

indicated in the Data Sheet and the factors used for the selection of the Bidder should take the likelihood of continuation into account. It will be the exclusive decision of the Client whether to have the downstream assignment carried out, and if it is carried out, which Bidder will be hired for the purpose.

1.6. It is BMTC's policy to require that Bidders observe the highest standard of ethics during the execution of such contracts. In pursuance of this policy, the BMTC:

1.6.1. defines, for the purposes of this provision, the terms set forth below as follows:

1.6.1.1. "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the

1.6.1.2. "Fraudulent practice" means a misrepresentation of facts in order to influence a selection process or the execution of a contract to the detriment of BMTC, and includes collusive practices among Bidders (prior to or after submission of proposals) designed to establish prices at artificial, non-competitive levels and to deprive BMTC of the benefits of free and open competition

1.6.2. will reject a proposal for award if it determines that the firm recommended for award has engaged in corrupt or fraudulent activities in competing for the contract in question;

1.6.3. will declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded BMTC/GoK-financed contract if it at any time determines that the firm has engaged in corrupt or fraudulent practices in competing for, or in executing, a BMTC/GoK-financed contract; and

1.6.4. Will have the right to require that, BMTC to inspect Bidder's accounts and records relating to the performance of the contract and to have them audited by auditors appointed by BMTC.

1.7. Bidders shall not be under a declaration of ineligibility for corrupt and fraudulent practices issued by BMTC in accordance with the above sub-Para 1.8.3

1.8. Bidders shall be aware of the provisions on fraud and corruption stated in the standard contract under the clauses indicated in the Data Sheet.

2. CLARIFICATION AND AMENDMENT OF RFP DOCUMENTS

2.1. Bidders may request a clarification of any item of the RFP document up to the number of days indicated in the Data Sheet before the Proposal submission date. Any request for clarification must be sent though the mode indicated in the Data Sheet. The Client will respond as per the mode indicated in the Data Sheet.

2.2. At any time before the submission of Proposals, the Client may, for any reason, whether at its own initiative or in response to a clarification requested by an invited firm, modify the RFP documents by amendment. Any amendment shall be issued in writing through addenda. Addenda shall be as per the mode mentioned in the Data Sheet. The Client may at its discretion

extend the deadline for the submission of Proposals.

3. PREPARATION OF PROPOSAL

3.1. Bidders are requested to submit a Proposal written in the language(s) specified in the Data Sheet.

A. TECHNICAL PROPOSAL

3.2. In preparing the Technical Proposal, Bidders are expected to examine the documents comprising this RFP in detail. Material deficiencies in providing the information requested may result in rejection of a Proposal. Only Proposed Technical details to be mentioned.

3.3. While preparing the Technical Proposal, Bidders must give attention to the following:

3.3.1. Alternative key professional staff shall not be proposed, and only one curriculum vita (CV) may be submitted for each position.

3.3.2. Reports to be issued by the Bidders as part of this assignment must be in the language(s) specified in the Data Sheet. It is desirable that the firm's personnel have a working knowledge of the Kannada & English language.

3.4. The Technical Proposal should provide the following information using the attached Standard Forms (Section 3):

3.4.1. Any comments or suggestions on the Terms of Reference and on the data, a list of services, and facilities to be provided by the Client.

3.4.2. A description of the methodology and work plan for performing the assignment.

3.4.3. The list of the proposed staff and the tasks that would be assigned to each staff,

3.4.4. Any additional information requested in the Data Sheet.

3.5. The Technical Proposal shall not include any financial information.

3.6. Conditions to RFP requirement/deviation to the requirements regarding scope of work, duration, SLA to be mentioned separately.

B. FINANCIAL PROPOSAL

3.7. In preparing the Financial Proposal, Bidders are expected to consider the requirements and conditions of the RFP documents. The Financial Proposal should follow Standard Forms (Section 4). It lists all costs associated with the Assignment, including (a) remuneration for staff, and (b) reimbursable such as subsistence (per diem, housing), transportation (national and local, for mobilization and demobilization), services and equipment (vehicles, office equipment, furniture, and supplies), insurance, printing of documents, surveys; and training, if it is a major component of the assignment. If appropriate, these costs should be included while submitting the proposal as integrated cost of the financial proposal.

3.8. Bidders shall express the price of their services in Indian Rupees.

3.9. The Data Sheet indicates how long the proposals must remain valid after the submission date. During this period, the Bidder is expected to keep available the key professional staff proposed for the assignment. The Client will make its best effort to

complete negotiations within this period. If the Client wishes to extend the validity period of the proposals, the Bidders who do not agree have the right not to extend the validity of their proposals.

4. SUBMISSION, RECEIPT, AND OPENING OF PROPOSALS

4.1. The Bidders shall upload the Response to RFP through e – procurement system only. No other mode of submission is permitted.

4.2. The representative's authorization is confirmed by a Power of Attorney accompanying the Proposal.

4.3. Bidder shall prepare a Pre-Qualification Criteria compliance document against each of the serial numbers of the PQ/Eligibility Criteria Bid Evaluation given.

4.4. Any Proposal received after the closing time for submission of proposals shall not be considered for evaluation.

4.5. The Financial Bids will be opened only for those Bidders who are declared as qualified in Pre-qualification/Eligibility Criteria Evaluation.

4.6. The date and time for opening of financial bid shall be made available to the qualified Bidder through e-procurement portal.

5. PROPOSAL EVALUATION

A. GENERAL

5.1. From the time the proposals are opened to the time the contract is awarded, if any Bidder wishes to contact the Client on any matter related to its proposal, it should do so as per the method indicated in the Data Sheet. Any effort by the firm to influence the Client in the Client's proposal evaluation, proposal comparison or contract award decisions may result in the rejection of the Bidder's proposal.

5.2. Evaluators of Pre-qualification/Eligibility Criteria Proposals shall have no access to the Financial Proposals until the Pre-qualification/Eligibility Criteria evaluation.

B. EVALUATION OF PRE-QUALIFICATION/ELIGIBILITY CRITERIA PROPOSALS

5.3. The evaluation committee appointed by the Client as a whole, and each of its members individually, evaluates the proposals based on their responsiveness to the Terms of Reference, applying the evaluation criteria specified in the RFP. A proposal shall be rejected at this stage if it does not respond to important aspects of the Terms of Reference.

C. OPENING AND EVALUATION OF FINANCIAL PROPOSALS; RANKING;

5.4. After the evaluation of qualifying criteria is completed, the Client shall notify through e-procurement portal whose proposals did not meet the minimum qualification were considered non-responsive to the RFP/RFP and TOR. The Bidder shall refer to the e-procurement website for the opening of financial bids.

5.5. The Financial Proposals shall be opened in e-procurement portal,

the evaluation committee will determine whether the Financial Proposals are complete and correct and if there are any computational errors

6. NEGOTIATIONS

6.1. Negotiations will be held at the address indicated in the Data Sheet. The aim is to reach agreement on all points and sign a contract.

6.2. Negotiations will include a discussion of the Technical Proposal, the proposed methodology (work plan), staffing and any suggestions made by the firm to improve the Terms of Reference. The Client and Bidder will then work out final Terms of Reference, staffing, and bar charts indicating activities, staff, periods in the field and in the home office, staff-months, logistics, and reporting. The agreed work plan and final Terms of Reference will then be incorporated in the "Annexure –A: Description of Services" and form part of the contract. Special attention will be paid to getting the most the Bidder can offer within the available budget and to clearly defining the inputs required from the Client to ensure satisfactory implementation of the Assignment.

6.3. Before contract negotiations, the Client will require assurances that the experts will be available. The Client will not consider substitutions during contract negotiations unless both parties agree that undue delay in the selection process makes such substitution unavoidable or that such changes are critical to meet the objectives of the assignment.

6.4. The negotiations will conclude with a review of the draft form of the contract. To complete negotiations, the Client and the Bidder will initial the agreed contract. If negotiations fail because the lowest price is higher than the customer budget, the Client can cancel the RFP and can go for Recall.

7. AWARD OF CONTRACT

7.1. The Client will promptly notify the award of the Bid in the e-Procurement portal.

7.2. The Bidder is expected to commence the assignment on successful issue of LOI / work order.

7.3. The bidder shall sign the agreement after providing performance bank guarantee.

8. CONFIDENTIALITY

8.1. Information relating to evaluation of proposals and recommendations concerning awards shall not be disclosed to the Bidders who submitted the proposals or to other persons not officially concerned with the process, until the winning Bidder has been notified that it has been awarded the contract.

9. DATA SHEET

Clause Reference	
1.1	**The client's name:** Bangalore Metropolitan transport

Clause Reference	
	Corporation **The method of selection**: Lowest Cost Selection (LCS)
1.2	Financial Proposals are requested: Yes The **Name, Objectives and Description** of the Assignment are provided in Terms of Reference
1.4	A pre-proposal conference will be held: Yes Date, Time and Venue: RFP Schedule Official Contact: RFP Schedule
1.5	BMTC will provide the following inputs: I. Terms of Reference (TOR) II. Any other clarifications and the necessary changes in the TOR for effective implementation of the assignment. III. Details of Infrastructure, departments and current processes
1.6	• The EMD amount will be forfeitted if bidder withdraw or modify their bids during bid validity period, bidder will be suspended for part of any tendering process in state of Karnataka for period of 1 year from the date of notice issued. • The bidder, by submitting its Proposal pursuant to this RFP, shall be deemed to have acknowledged that without prejudice to BMTC's right or remedy herein under or in law or otherwise, o If a bidder withdraws their bid or increases their quoted prices during the period of bid validity or its extended period, if any. o In the case of a successful bidder if the bidder fails to sign the Contract or to furnish Performance Bank Guarantee/Security Deposit within specified time. o During the bid process, if a bidder indulges in any such deliberate act as would jeopardize or unnecessarily delay the process of bid evaluation and finalization. o Deliberate attempts by the bidder to share wrong information / manipulate information / hide the facts.
1.10	The clauses on fraud and corruption in the contract are mentioned in GCC Sub-Clause 2.7.1
2.1	Bidder may request a clarification of any item of the RFP document as per the timeline specified in the RFP schedule. Any request for clarification/ Pre-Bid Queries must be uploaded online in the e-Procurement portal https://kppp.karnataka.gov.in.The Client will respond to such requests by uploading in the e-procurement portal (including an explanation of the query but without identifying the source of inquiry)
3.1.	Proposals should be submitted in the following

Clause Reference	
	language(s): English
3.4	Training is an important feature in the assignment: Yes
3.8.	Proposals must remain valid for 90 days after the submission date
4	• Proposals should be uploaded as per schedule in RFP schedule. • The Proposal, and its copy, shall be typed or written in indelible ink and signed by the authorized signatory of the bidder who shall initial each page, in blue ink. In case of printed and published documents, only the cover shall be initialled. All the alterations, omissions, additions, or any other amendments made to the Proposal shall be initialled by the person(s) signing the Proposal. The Proposals must be properly signed by the authorized representative (the "Authorized Representative") as detailed below: a) by a partner, in case of a partnership firm and/or a limited liability partnership; or b) by a duly authorized person holding the Power of Attorney, in case of a Limited Company or a corporation; or c) by the Authorized Representative of the Lead Member, in case of consortium. • A copy of the Power of Attorney certified under the hands of a partner or director of the Applicant and notarized by a notary public in the form specified in RFP Document shall accompany the Proposal. • Proposals shall remain valid at a minimum for the period specified in the Data Sheet after the Proposal Due Date prescribed by BMTC. A Proposal valid for a shorter period shall be rejected by BMTC as non-responsive. • In exceptional circumstances, prior to expiry of the Proposal validity period, BMTC may request that the Bidders extend the period of validity for a specified additional period. The request and the responses to the request shall be made in writing. A bidder agreeing to the request will not be required or permitted to modify its Proposal but will be required to ensure that the EMD is extended for a correspondingly longer period. • **Electronic Proposal Submission:** Detailed guidelines for viewing Proposals and submission of online Proposals are given on the website. The Invitation for Proposals is published on this website. Bidder can logon to this website and view the Invitation for Proposals and can view the details of works for which Proposals are invited. The prospective bidder shall submit Proposals online; for this, the

Clause Reference	
	bidder is required to have enrolment/registration in the website and should have valid Digital Signature Certificate (DSC) Keys. The DSC can be obtained from any authorized certifying agencies. The bidder should register in the web site https://kppp.karnataka.gov.in . After this, the bidder can login the site through the secured login. **Note:** BMTC shall not be responsible for any technical issues pertaining to internet connectivity, browser compatibility and any other technical issues pertaining to uploading of bid documents in e-procurement portal. The Bidders are requested to upload their Proposals in e-portal well in advance to avoid non-availability of internet connection.
5.1.	• Any queries should be submitted as mentioned in the Datasheet. Further details on communication are mentioned in the RFP Schedule. • The Bidder shall quote the prices as specified in the format given in Financial Proposal format. • All prices should be clearly written both in figures and in words. Bidders should ensure that there are no alterations / corrections in the quotes submitted by them. • In case of a discrepancy between the prices in figures and words, the prices in lowest will be considered as correct. • The prices quoted shall be firm throughout the period of the validity of the offer and subsequently during the currency of the contract and shall not be subject to any variation/revision.
5.2.	• BMTC shall constitute a Tender Scrutiny Committee to evaluate the Pre-qualification of the bidders. The Tender Scrutiny Committee shall evaluate the responses to the RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids. • The Committee may seek inputs from their professional and technical experts in the evaluation process. • BMTC reserves the right to do a reference check of the past experience stated by the bidder. Any feedback received during the reference check shall be considered during the evaluation process. • The decision of the Tender Scrutiny Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. • The Tender Scrutiny Committee reserves the right to reject any or all bids. Each of the responses shall be

Clause Reference	
	evaluated as per the criteria and requirements specified in this RFP.
5.3.	Details on the Eligibility Criteria can be found in **Section 5: Terms of Reference**
6.1	The Address of Communication is mentioned in RFP Schedule
7.1	• The Performance Security/Security Deposit shall be provided by the successful bidder no later than the date specified in the Letter of Acceptance and shall draw a Demand Draft (DD) in favour of "The CAO-FA, BMTC, Bengaluru" or an unconditional Bank Guarantee (BG) from any of the Nationalized Banks or Public Sector Banks in favour of the "Controller of Stores and Purchases, BMTC, Bangalore" • The BG/DD shall be furnished for an amount equivalent to 10%of the contract value • The Bank guarantee shall be valid 06 months from the Intended date of Completion of the project Period. If the project duration gets extended, the performance security shall be valid until 180 days from the new date of completion of project. • The MSP shall keep the Performance Bank Guarantee valid and enforceable throughout the Term and for a period of 180 days after the Term. In case the Performance Bank Guarantee provided by the MSP to BMTC is set to expire for any reason whatsoever at any time before expiry of 60 days after the Term, the MSP shall renew and provide to BMTC renewed Performance Bank Guarantee at least 60days prior to its date of expiry. Upon any failure on part of the MSP to renew the Performance Bank Guarantee or to keep it valid and enforceable in terms of this Clause, the Performance Bank Guarantee will be en-cashed by BMTC without giving any notice to the MSP or to any other Party. • There will be no interest on the Security Deposit amount • This is without prejudice to any other action that may be taken by BMTC under the terms and conditions of this Contract. • BMTC, without prejudice to any of its rights or remedies under this Contract, is free to en-cash the Performance Bank Guarantee in part or in full, in terms. In the event of the invocation of any amount of the Performance Bank Guarantee by BMTC under the Contract, the MSP shall immediately take appropriate steps to establish the Performance Bank Guarantee at its full value contemplated under the Contract within 15 days of the date when the

Clause Reference	
	Performance Bank Guarantee is wholly or partially invoked by BMTC • Right to vary the scope of the work at the time of award: BMTC reserves its right to make changes to the scope of the work at the time of execution of the resultant Agreement • Right to accept any bid and reject any or all bids BMTC reserves the right to accept or reject any Bid, and to annul the tendering process and reject all tenders at any time prior to award of contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for such action. • Right to termination/cancellation: Notwithstanding anything contained in this document, BMTC, reserves the right to cancel/ terminate the bid/offer process without assigning any reason whatsoever, at any time, prior to signing of the contract with no liability **Payment and SLAs** Details provided in the Terms of Reference
9	**Dispute Resolution:** Any Dispute arising during Contract Period between the parties shall be resolved amicably without adversely impacting Project Implementation and Operation.
10	**Insolvency and Breach** BMTC may at any time, by notice in writing summarily terminate the contract without compensation to the bidder in any of the following events, if the bidder: a) If a firm, any partner thereof, shall at any time, be adjudged insolvent or shall have a receiving order or order for administration of his estate made against him or shall take any proceeding for composition under any Insolvency Act for the time being in force or make any conveyance or assignment of his effects or enter into any assignment or composition with his creditors or suspend payment or if the firm be dissolved under the Partnership Act, or b) Being a company is wound up voluntarily or by the order of a court or a Receiver, Liquidator, or Manager on behalf of the debenture holders is appointed, or circumstances shall have arisen which entitle the Court or debenture holders to appoint a Receiver, Liquidator or Manager, or c) Commits any breach of the contract not herein specifically provided for. Provided always that such determination shall not prejudice any right of action or remedy which shall have accrued or shall accrue

Clause Reference	
	thereafter to BMTC and provided also the bidder shall be liable to pay to BMTC any extra expenditure he is thereby put to and the bidder shall, under no circumstances, be entitled to any gain on repurchase.

Sincerely,

SECTION 3: PROPOSAL SUBMISSION – STANDARD FORMS

1. PROPOSAL SUBMISSION FORM

[Location, Date]

FROM: (Name of Bidder)
To:(Name of Authority)
Madam/Sir:

Subject: **"SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC"**
Tender No. BMTC/2023-24/SE0074 Date:14.06.2023.

1. We, the undersigned, offer to provide the services for the above in accordance with your Request for Proposal dated [Date], and our Proposal. We are hereby submitting our Proposal which includes the Pre-Qualification Proposal and Financial Proposal through e-procurement and hard copies submission of Qualification Proposal.

2. We hereby declare that all the information and statements made in this Proposal are true and accept that any misinterpretation contained in it may lead to our disqualification.

3. We have read the provisions of the RFP Document and confirm that these are acceptable to us. We further declare that additional conditions, variations, deviations, if any, found in our proposal shall not be given effect to.

4. We shall pay the EMD Amount.

5. We understand you are not bound to shortlist / accept any proposal you receive.

Address of responding Company
Name, Designation and Address of the contact
Authorized Person, with details of Phone nos.,
Telephone/Mobile No of Contact Person
E-Mail ID

We remain,
Yours sincerely,
Name and Title of Signatory:
Name of Firm:
Address:

2. CHECKLIST

(To be submitted along with Proposal Submission Form)

Sl.	Proposal Requirement	Compliance (Yes/No)
1	Earnest Money Deposit	
2	Certificates of incorporation/Registration Certificates along with Bylaws/MoA&AoA or similar legal document	
3	GST Registration of MSP	
4	Copy of PAN Card of MSP	
5	Certificate of Incorporation / Registration of the proposed CSP	
6	Copy of GST registration of the proposed CSP	
7	Copy of PAN Card of the proposed CSP	
8	MSP: Audited financial statements for last three Financial Years along with CA certificate clearly specifying turnover (2019-20, 2020-21 and 2021-22).	
9	CSP: Audited financial statements along with CA certificate clearly specifying turnover [for any three (3) financial years, out of last five (5) years for cloud business in India (2017-18, 2018-19, 2019-20, 2020-21, 2021-22)]	
10	Letter of support/ Authorization Letter from the CSP to the Bidder for providing services for this particular Project.	
11	Copy of Client certificate, work order, completion certificate or extract from the contract mentioning the scope of work indicating that the bidder has executed or a concurrent project of similar nature.	
12	Letter of Empanelment issued by MEITY	
13	Self-declaration of CSP/Copy of certificates regarding proposed CSP able to provide IAAS, PAAS and SAAS as and when required by the department	
14	Self-declaration of CSP regarding propose CSP have data centres in India as per MeiTy Guidelines	
15	Self-certificate issued on the CSP letterhead and relevant copy of the certificates: • SOC1, SOC2 • PCI DSS Level 1 • ISO 27017 • ISO 27018 • ISO 20000 • ISO 27001 • ISO Certificates for 'Business Continuity and Resilience' and 'Privacy Management (PII)': ISO 22301 and ISO 27701	
16	Self-declaration by the bidder duly notarized and signed by the authorized signatory regarding bidder not have been blacklisted by any Central / State	

	Government Department / PSU in India as on the bid submission date.	
17	Self-declaration by the Bidder duly notarized and signed by the authorized signatory regarding bidder not have been declared bankrupt or in the process of insolvency proceedings.	
18	Self-Declaration indicating proposed CSP not having been blacklisted by any Government Agency in India as on Bid submission date by the authorized signatory of the CSP on company's letterhead.	
19	Documents/Certificates/ Endorsement from the Cloud Provider with public link on CSP website, regarding CSP have an Underlying Hypervisor Capability which can support 1:1 or 1:2 Physical Core to Virtual Core Ratio.	
20	Self-Certificate issued on the CSP letterhead along with supporting document of public facing website regarding cloud services rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across data centre and outage details (if any) with Root Cause Analysis (RCA)	
21	Self-Certificate issued on the CSP letterhead along with supporting document of having market place solutions with first and 3rd party products and services to be used as services on their cloud platform	
22	Description of Approach, Methodology, work plan and Technical Specifications document	
23	CV of proposed key personnel	
24	Proposal Submission Form	
25	Qualification Submission Form	
26	Declarations	
27	Power of Attorney for signing the proposal	
28	Checklist for mandatory Requirements of proposed CSP	
29	Conditions to RFP requirement/deviation to the requirements regarding scope of work, duration, SLA to be mentioned	

3. QUALIFICATION SUBMISSION FORM

Prospective bidders shall submit information in the following format in the uploaded bid

	Description					**Documents to be Attached**
1	The Bidder, as a single legal entity, must be registered in India and should have been in operations in India for a minimum of three (3) years by the date of opening of the bid.					Certificate of incorporation/ Registration Certificates along with Bylaws/MoA&AoA or similar legal document & GST Registration Copy of PAN Card
2 a.	Bidder must have minimum average turnover of **INR 30 Crores** for the last three (3) Financial Years (2019-20, 2020-21 and 2021-22).					
FY	2019-20	2020-21	2021-22			Audited financial statements for last three Financial Years along with CA certificate clearly specifying turnover.
2 b.	Bidder must propose CSP who should have annual turnover of **more than 300 Crores**, for any three (3) financial years, out of last five (5) years for cloud business in India (2017-18, 2018-19, 2019-20, 2020-21, 2021-22)					
	2017-18	2018-19	2019-20	2020-21	2021-22	Audited financial statements along with CA certificate clearly specifying turnover.
3	The Bidder should be authorized by the proposed CSP to participate in the bid and shall provide services only from that CSP under this bid.					Letter of support/ Authorization Letter from the CSP to the Bidder for providing services for this particular Project.
4	Bidder should have executed at least two cloud related projects each of INR 2 Crores or higher from a State/Central/PSU/private Departments/ firms in India.					Copy of Client certificate, work order, completion certificate or extract from the contract mentioning the scope of work.

No	Project	Duration From: To:	Name of Client & Country of eligible assignment	Role of Bidder	Value of the Project	Status (Completed/ Ongoing)	Certificate from the client provided
(Purchase Order / Work Order / Completion certificate from client / statutory auditor certificate in English to be enclosed)							

5 a	Bidder must propose CSP which is STQC audited and MEITY	Letter of Empanelment issued by MEITY

	empanelled	
5 b	Bidder must propose CSP who must be able to provide IAAS, PAAS and SAAS as and when required by the department	Self-declaration of CSP/Copy of certificates
5c	Bidder must propose CSP who should have data centres in India as per MeiTy Guidelines	Self-declaration of CSP.
6	The Bidder should propose services from a CSP with the following valid certificates: SOC1, SOC2 PCI DSS Level 1 ISO27017 ISO27018 ISO20000 ISO 27001 ISO Certificates for 'Business Continuity and Resilience' and 'Privacy Management (PII)': ISO 22301 and ISO 27701	Self-certificate issued on the CSP letterhead and relevant copy of the certificate.
7	The bidder should not have been blacklisted by any Central / State Government Department / PSU in India as on the bid submission date.	Self-declaration by the bidder duly notarized and signed by the authorized signatory on Non – judicial stamp paper of INR 100/-
8	The bidder should not have been declared bankrupt or in the process of insolvency proceedings.	Self-declaration by the Bidder duly notarized and signed by the authorized signatory on Non – judicial stamp paper of INR 100/-
9	CSP must have an Underlying Hypervisor Capability which can support 1:1 or 1:2 Physical Core to Virtual Core Ratio	Documents/Certificates/ Endorsement from the Cloud Provider with public link on CSP website.
10	CSP shall have published on its public facing website- cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across datacentre and outage details (if any) with Root Cause Analysis (RCA)	Self-Certificate issued on the CSP letterhead along with supporting document of public facing website regarding cloud services rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across data centre and outage details (if any) with Root Cause Analysis (RCA)
1	Cloud Service Provider should offer	Self-Certificate issued on

1	Market Place solutions with first and 3rd party products and services to be used as services on their cloud platform	the CSP letterhead along with supporting document of having market place solutions with first and 3rd party products and services to be used as services on their cloud platform

- For each eligible assignment, the bidder should indicate the duration of the assignment, the contract amount, the amount paid to the bidder and the bidder's role/involvement.
- Bidders are expected to provide information in respect of each eligible assignment in this Appendix. Each eligible assignment must comply with the requirements set out in the Data Sheet.
- For each completed eligible assignment, work order **OR** the completion certificate issued by the client certifying that the assignment has been completed by the bidder should be furnished
- For each ongoing Eligible Assignment, the work order and certificate issued by the client certifying the percentage of completion of the assignment by the bidder should be furnished.
- The client reserves the right to ask for documentary proofs for the claims made with regard to technical eligibility and work experience at any stage of bid process or for the selected bidder, any time thereafter.
- The client reserves all rights to verify the authenticity of experience related certificates or any other certificates submitted by the bidder, at any stage of bid process or even thereafter. In case of finding any fraudulent practice during verification, the client shall reject the bid or terminate the contract.

4. CERTIFICATE FROM THE STATUTORY AUDITOR REGARDING TURNOVER- MSP

(On the letter head of the statutory auditor)

Based on its books of accounts and other published information authenticated by it, this is to certify that the turnover of …… (Name of the Bidder) for the Financial Year 2019-20, 2020-21 and 2021-22 is as follows:

Sl.	**Financial Year**	**Annual Turnover (INR Cr.)**
1.	Year 2019–20	
2.	Year 2020–21	
3.	Year 2021–22	

Name of the audit firm:
Seal of the audit firm:

Signature:
Name:
Membership Number:
Designation:
Date:

5. CERTIFICATE FROM THE STATUTORY AUDITOR REGARDING TURNOVER- CSP

(On the letter head of the statutory auditor)

Based on its books of accounts and other published information authenticated by it, this is to certify that the turnover of …… (name of the Bidder) for the Financial Year 2017-18, 2018-19, 2019-20, 2020-21, 2021-22 is as follows:

Sl. No.	Financial Year	Annual Turnover (INR Cr.)
1.	Year 2017 – 18	
2.	Year 2018– 19	
3.	Year 2019–20	
4.	Year 2020– 21	
5.	Year 2021–22	

Name of the audit firm:
Seal of the audit firm:
Signature:
Name:
Membership Number:
Designation:
Date:

6. DECLARATION

(Proforma of Declaration to be furnished on a Government Stamp Paper of value as prescribed by BMTC)

The Controller of Stores & Purchase,
BMTC, Central Offices,
K.H. Road, BANGALORE – 560 027

Sir,

Sub: "SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC"

Ref: Tender No: BMTC/2023-24/SE0074 Date:14.06.2023

We hereby declare that the rates quoted by us in lowest and we have not quoted/supplied the materials/provided service to any other STU/Organization during the preceding One year at less than the rates offered by us in the subject tender.

OR

We have supplied the materials/provided service to our following customers during the preceding One year at less than the rates offered to you in the subject tender, and the details are as follows:

Name of the STU / Organization to whom the supplies were made.
Rates offered to them
The reasons for variation
Quantity offered/supplied

We agree to abide by the payment clause of the tender. We agree to abide by all the terms and conditions of the tender and fulfil all the requirements mentioned in the Tender. We are aware that in case of any conditional offer submitted by us in respect of any payment and other terms and conditions of tender our offer is liable to be rejected.

The amount quoted in the Commercial bid of e-procurement portal is final and we agree to hold the same till the completion of the service.

Signature of the Authorized Signatory,
Designation, Date
Seal of the Company

7. FORMAT FOR POWER OF ATTORNEY FOR SIGNING OF PROPOSAL

(On Non – judicial stamp paper of Rs 100/- or such equivalent amount and document duly attested by notary public)

Power of Attorney

Know all men by these presents, we ..... (Name of the Bidder and address of the registered office) do hereby constitute, appoint and authorize Mr. / Ms..... ..... (name and residential address) who is presently employed with us and holding the position of ..... as our true and lawful attorney (hereinafter referred to as the "attorney"), to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to submission of our Proposal for **"SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR PROVISION OF CLOUD SERVICES TO BMTC"** of [Name of THE AUTHORITY], including signing and submission of the Proposal and all accompanying documents, attending the pre-bid meeting, providing information/responses to [Name of THE AUTHORITY], representing us in all matters before [Name of THE AUTHORITY], if selected, undertaking negotiations with [Name of THE AUTHORITY] prior to the execution of the Contract and generally dealing with [Name of THE AUTHORITY] in all matters in connection with our Proposal.

We hereby agree to ratify and confirm and do hereby ratify and confirm all acts, deeds and things done or caused to be done by our said attorney pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our attorney in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, THE ABOVE-NAMED PRINCIPAL HAVE EXECUTED THIS POWER OF ATTORNEY ON THIS ..... DAY OF ....., 20.....

For _____
(Signature)
(Name, Title and Address)

Accepted
..... (Signature)
(Name, Title and Address of the Attorney)

The mode of execution of the power of attorney should be in accordance with the procedure, if any, lay down by the applicable law and the charter documents of the executants(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

In case the Proposal is signed by an authorized director of the Bidder, a certified copy of the appropriate resolution/ document conveying such THE AUTHORITY may be enclosed in lieu of the power of attorney.

For a power of attorney executed and issued overseas, the document will have to be notarized in the jurisdiction where the power of attorney is being issued.

8. COMMENTS AND SUGGESTIONS OF BIDDER

On the Terms of Reference

1.
2.
3.
4.
5.

On the data, services, and facilities to be provided by BMTC

1.
2.
3.
4.
5.

9. DESCRIPTION OF APPROACH, METHODOLOGY, WORK PLAN AND TECHNICAL SPECIFICATIONS

Technical approach, methodology and work plan are the key components of the Technical Proposal. You shall present your Technical Proposal divided into the following four chapters:

a. **Technical Approach and Methodology:**
In this chapter the bidder should explain their understanding of the objectives of the assignment.

b. Detail Implementation and Maintenance Plan
In this chapter the bidder should propose the main activities of the assignment, their content and duration. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the TOR and ability to translate them into a feasible working plan. A list of the final documents, including reports,

drawings, and tables to be delivered as final output, should be included here.

c. Technical Specifications of proposed cloud solution

In this chapter the bidder should mention the detailed technical specifications of the proposed cloud components. These should be compliant to the Scope of Work and Mandatory Requirements mentioned in **Section 5: Terms of Reference.**

d. **Technical Proposal document comprising of**:

- Overall Cloud architecture including solution design
- Project Management and Implementation Methodology
- Cloud Migration Approach and methodology
- Disaster Recovery and Business Continuity approach
- Integration approach with other IT Infrastructure
- Maintenance and Support for proposed solution
- Risk and Mitigation plan
- Details of statistics of availability of services from CSP.

10. FORMAT FOR CURRICULUM VITAE (CV) OF PROPOSED MANPOWER

The Bidder shall provide the Curriculum Vitae of the proposed manpower in the format given below:

<table>
<tr><td>1.</td><td>Name of the Staff</td><td></td></tr>
<tr><td>2.</td><td>Current Designation in the Organization</td><td></td></tr>
<tr><td>3.</td><td>Proposed Role in the Project</td><td></td></tr>
<tr><td>4.</td><td>Proposed Responsibilities in the Project</td><td></td></tr>
<tr><td>5.</td><td>Date of Birth</td><td></td></tr>
<tr><td>6.</td><td>Educational Qualifications</td><td><Degree>/<Diploma>, <College/University>, <Year of Passing></td></tr>
<tr><td>7.</td><td>Key Training and Certifications</td><td></td></tr>
<tr><td>8.</td><td>Language Proficiency</td><td><table><tr><td>Language</td><td>Reading</td><td>Writing</td><td>Speaking</td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

<table>
<tr><td>9.</td><td>Employment Record
(For the Total Relevant Experience)</td><td><table><tr><td>From / To:</td><td>Employer</td><td>Position Held</td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>10.</td><td>Total No. of Years of Work Experience</td><td></td></tr>
<tr><td>11.</td><td>Total No. of Years of Experience for the Role Proposed</td><td></td></tr>
<tr><td>12.</td><td>Highlights of relevant assignments handled and significant accomplishments</td><td>Use following format for each project<table><tr><td>Name of Assignment/Project:</td><td></td></tr><tr><td>Year:</td><td></td></tr><tr><td>Location:</td><td></td></tr><tr><td>Client:</td><td></td></tr><tr><td>Main Project Features:</td><td></td></tr><tr><td>Positions Held:</td><td></td></tr><tr><td>Activities Performed:</td><td></td></tr></table></td></tr>
</table>

11. FORMAT FOR AFFIDAVIT CERTIFYING THAT BIDDER IS NOT BLACKLISTED

I M/s. …… , (the name of the Bidder and addresses of the registered office) hereby certify and confirm that we or any of our promoter/s/chief executive officer/ directors/managers are not barred or blacklisted by any government or government instrumentality or public sector organization in India or in any other jurisdiction to which we or our Affiliates belong or in which we or our Affiliates conduct business from participating in any project or being awarded any contract, either individually or as member of a consortium and no such bar or blacklisting subsists as on the Proposal Due Date.

We further confirm that we are aware our Proposal for the "**SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC"** would be liable for rejection in case any material misrepresentation is made or discovered with regard to the requirements of this RFP at any stage of selection and/or thereafter during the term of the Contract.

Dated this …… Day of ……., 20….
Name of the Bidder……
Signature of the Authorized Person ……
Name of the Authorized Person

12. DECLARATION ON NO BANKRUPTCY/INSOLVENCY

(Proforma of Declaration to be furnished duly notarized and signed by the authorized signatory on Non – judicial stamp paper of INR 100/-)

This is to certify that the bidding entity is <company name>, engaged in providing <type of services>.

I, <name of signatory>, <designation>, do hereby declare to the best of our knowledge and information available with us on <bid submission date dd/mm/yyyy>, that <company name> has not been declared bankrupt or in the process of insolvency proceedings.

Signature of the Authorized Signatory
Designation, Date, Seal of the Company

13. DECLARATION REGARDING RESTRICTIONS ON PUBLIC PROCUREMENTS FROM BIDDERS OF COUNTRIES WHICH SHARES A LAND BORDER WITH INDIA:

Compliance Certificate regarding restrictions on public procurements from bidders of countries which shares a Land Border with India

(to be furnished on a Government Stamp Paper of Rs. 100/-)

The Controller of Stores and Purchases
BMTC, Central Offices, K.H. Road,
Bengaluru-560 027

Sir,

Sub: SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC
Tender No: BMTC/2023-24/SE0074 Date:14.06.2023.

*****

We have read the clauses regarding restrictions on procurement from a bidder of a country which shares a land border with India (GoI Letter No. F.No. 6/18/2019 -PPD dtd: 23.07.2020 Order (Public Procurement No. 1 and 2) dated 23.07.2020 & Order (Public Procurement No. 3) dated 24.07.2020 and GO of GoK vide No. FD 455 Exp-12 2020 Bengaluru Dated:25.08.2020. **GoI OM vide No.F.No.18/37/2020-PPD dtd: 08.02.2021 and GoK circular vide No.FD 455 Exp-12/2020 Bengaluru Dtd: 10.03.2021.**

i. I/ Wecertify that, we arenot from such a country which shares a land border with Indiaand we are eligible to be considered.

Or

I/ We declare that, we are from such a countryor countries which shares a land border with Indiaand we have been registered with the Competent Authority and certify that, we fulfill all requirements in this regard and are eligible to be considered. A copy of the valid registration by the Competent Authority is enclosed along with this declaration for Evidence.

ii. We declare that, we will not sub-contract any work to a contractor from such country or countries which shares a land border with India unless such contractor is registered with the Competent Authority in case the work order is released on us. We fulfill all requirements in this regard and is eligible to be considered.(A copy of the valid registration issued by the Competent Authority to be enclosed if applicable).

iii. We declare that, we will not supply finished goods procured directly/ indirectly from the vendors from the countries sharing land border with India unless such vendor is registered with the Competent Authority.

iv. We aware of the fact that, ifthe information provided byus in this certificate/ declaration is found to be false at any stage, this would be a ground for immediate termination of order/ contract/ LoIand further legal action against us in accordance with law.

v. We are aware that, such registration with Competent Authority should be valid at the time of submission of bids and at the time of acceptance of bids.

Signature of the Authorized Signatory.
Name:
Designation:
Mobile No:
E-Mail ID:
Date:
Seal of the Company

14. CHECKLIST FOR MANDATORY REQUIREMENTS OF PROPOSED CSP

Sl. No.	Description	CSP Offering (Y/N)
1	**Compute Service:** a) Compute instances offered should be **latest generation processor.** b) **Physical core to vCPU ratio should not more than 1:2** for the proposed VMs as well as for additional VMs required during contract period. c) Self-service provisioning of multiple VMs concurrently either through a programmatic interface or Web Portal on Cloud. d) Should be able to schedule maintenance events for VM's such as a reboot, stop/start, or retirement. e) Ability to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance. f) Pause and Resume VMs (Hibernate compute instances when not required and resume them from this state at a later time). g) Ability to place instances in multiple distinct locations/ separate availability zones to protect applications from failure of a single location. h) All compute VMs must be on x64 platform only. i) **Support for Operating Systems:** Linux, Suse Linux Enterprise, RHEL (Red Hat Enterprise Linux), Windows. **j) Uptime SLA of 99.99% in Proposed CSPs India region.**	
2	**Block Storage** a) Self-service provisioning of storage either through a programmatic interface or Web Portal. b) **Ability to increase the size of an existing block storage volume** without having to provision a new volume and copy/move the data. c) Ability to dynamically increase capacity, tune performance, and change the type of live volumes with no downtime or performance impact. d) Supports point-in-time snapshots that are incremental in nature to speed up provisioning and recovery. e) Offers server-side encryption of data **'at-rest',**	

	i.e**., data stored on volumes and snapshots.** f) Ability to provide a simple, automated way to back up data stored on volumes by ensuring that snapshots are created and deleted on a custom schedule. User should no longer need to use scripts or other tools to comply with data backup and retention policies. g) Ability to provide **seamless encryption of data volumes**, boot volumes and snapshots, eliminating the need to build and manage a secure key management infrastructure. **h) Uptime SLA of 99.99% in Proposed CSPs India region.** i) CSP Should offer choice of block storage built of different physical drives such as SSD's, SAS drives etc. and also provide with desired performance capabilities.	
3	**Object Storage** a) Self-service provisioning of storage either through a programmatic interface or Web Portal b) Offer object storage tiering capability, i.e., the ability to recommend transitioning an object between object storage classes based on its frequency of access. c) Support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation to deletion. d) Ability to create and use policies to manage stored data, its lifecycle, and tiering settings. e) Capability to create policies that can restrict access to the data based on user/request location and time of request. f) Support hosting static websites out of its object storage service. g) **Support server-side encryption** (SSE) of data 'at-rest', **with the cloud provider managing the encryption keys or customer provided cryptographic keys.** h) Support read-after-write consistency for PUT operations for new objects. i) Support versioning, i.e., the ability to store and co-exist multiple versions of an object. j) Capability for a user to mark an item as undeletable. k) Provide multi factor authentication (MFA) and follow principle of least privilege. l) Ability to **send notifications when certain events happen at the object level** (i.e., addition/deletion operations) m) Capability of **generating audit logs that include details** about a single access request,	

	such as the requester, the request time, the request action, the response status, and the error code. n) Provider allow uploading an object as a set of parts where each part is a contiguous portion of the object's data and these objects parts can be uploaded independently and, in any order, o) Users the ability to retrieve only a subset of data from an object by using simple SQL expressions. p) Feature to block object version **deletion during a customer-defined retention period** so that you can enforce retention policies as an added layer of data protection or to meet compliance obligations. q) Must provide a mechanism to know who has access to the object store, as well as what level of access they have.	
4	**Network & Firewall** **a)** Capability to protect Cloud Infrastructure based on **protocols and ports.** b) Capability to protect network subnets with **access controls** that provides an optional layer of security that provides a **stateless firewall** for controlling traffic in and out of a subnet. **c)** Capability to **segregate public subnet and private subnet** d) Capability to **configure routes and filters** that define which subnets are allowed to route external traffic over backend VPN or site-site connections, Internet connections, or even specific virtual machine instances. e) **Prevent packet sniffing:** Virtual instances should be designed to prevent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. Even if tenants configure interfaces into promiscuous mode, the hypervisor should not deliver any traffic to them that is not addressed to them. f) **Prevent IP Spoofing:** the cloud service should not permit an instance to send traffic with a source IP or MAC address other than its own.	
5	**Implement Identity and Access Management (IAM)** to properly separate users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks**.** Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account.	

6	**Multi-factor authentication (MFA)** to prove physical possession of a hardware or virtual MFA device for accessing the console, as well as any privileged Identity and Access Management accounts associated with it.	
7	**Web Application Firewall:** Protection from attacks by filtering traffic based on rules that you create. Filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allow you to block common attack patterns, such as SQL injection or cross-site scripting that could affect application availability, compromise security, or consume excessive resources. Features like protection against Web Traffic visibility, east of deployment and maintenance, integrated security.	
8	**Distributed Denial of Service (DDoS) Protection:** Managed DDoS protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target web site or applications. When used with Content Delivery Network and global DNS service, should provide comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency.	
9	**Monitoring** a) **Monitoring Services for resources:** Capability to monitor cloud environment centrally, custom monitoring metrics, monitor and store logs, view graphs & statistics, set alarms, monitor and react to resource changes. Support monitoring of custom metrics generated by your applications and services and any log files your applications generate. Gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly. b) **Health Dashboard:** Provide alerts and remediation guidance when CSP is experiencing events that may impact the customer. Personalized view into the performance and availability of the Cloud services underlying your Cloud resources. c) **Proactive Advisory services:** Capability to analyse your Cloud environment and provide best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits.	
10	**Compliance** a) **Audit:** Capability to provide and record logs of all	

	user activity within a cloud environment including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the Cloud service. The API activity history should be delivered within a reasonable timeframe (<30 minutes) from the time API call is made. Capability to support storing log files in a durable and inexpensive storage solution. b) **Network logs:** Capability to capture information about the IP traffic going to and from network interfaces in your VPC that can be used to troubleshoot why specific traffic is not reaching an instance, or as a security tool to monitor the traffic that is reaching your instance. c) **Governance and Compliance:** Capability to discover all of cloud resources and view the configuration of each. Continuously monitor and record your Cloud resource configurations. Receive notifications each time a configuration changes, as well as dig into the configuration history to perform incident analysis. Capability to obtain details of what a resource's configuration looked like at any point in the past.	
11	**Certificate Authority:** Should be able to provide and manage **SSL certificates.**	

SECTION 4: FINANCIAL PROPOSAL

1. Price bids of only the Bidders who qualified the **Prequalification criteria will be evaluated. Contract will be awarded on the overall lowest cost (L1) basis.**
2. The bidder has to submit the financial proposal for the total project **duration of 48 months (4 years) in the e-procurement portal** and the quotation should consider the following costs:
   A. Cumulative **Bill of Materials of Cloud Services(as per configuration mentioned in section 5)**
   B. **O&M Phase Manpower Cost(as per resource profile given in Annexure 1)**

FORM 1: CALCULATION MATRIX FOR EVALUATION OF FINANCIAL BID

S. No	Particulars	Cumulative List Price	% Discount (as applicable)	Net Price	Total Price
1	Cumulative Bill of Materials of Cloud Services				A
2	O&M Phase Manpower Cost				B
Total Price=A+B					

Note to Bidder:

1. Bidders are required to **quote a discount percentage against** each of the following mentioned categories of services mentioned in the RFP.
2. **The %discount quoted for Cumulative Bill of Materials of Cloud Services will be applicable for each line item of rate discovery chart also.**
3. An indicative bill of materials of cloud services is provided in **Section 5**
4. The list price for each of the service will be multiplied by the indicated quantity and the cumulative list price shall be determined for the respective category of service.
5. The discount quoted/negotiated by the bidder for each service category will be applicable on all services falling in that service category.
6. All commercial quotation should include GST and any other tax if applicable
7. **The cloud services mentioned in section 5 are indicative only. If any service not mentioned in the BOQ (including any new cloud service introduced by the CSP after the tender due date),will have to be provided to BMTC at the same discount rate as quoted above under the respective service category. BMTC is also free to opt for any service or configuration of service in the host of offerings of the CSP at the same rate of discount.**

8. If mentioned configuration is of any of the item in **section 5**is not available in exact configuration then the next higher configuration will be considered for defining the list price and the uniform discount rate quoted shall be applicable.
9. The configuration mentioned in the below table is an indicative sizing based on **8 lakhs users and 6500 vehicle tracking devices.** The Bidder would be required to provide and comply with the following IT infrastructure and configuration.

FORM 2: BILL OF MATERIALS FOR CLOUD SERVICES

Bill of Material - Cloud Services - Reserved Instances												
Sl.	**Components**	**Total Qty**	**Cores**		**RAM**		**Storage**		**OS**	**Remarks**	**Usage for 4 years**	**Unit List Price**	**Total List Price**
		(Inclusive of HA) (X)	**Core Per VM**	**Total Cores**	**RAM (GB) per VM**	**Total RAM (GB)**	**Storage for each VM (GB)**	**Total Storage (In GB)**			**(Y)**	**(Z)**	**(X*Y*Z)**
1	BI Server (BOAP & Helpdesk - IMMS)	8	8	64	32	256	90	720	Windows	Active - Passive			
2	Web Servers (Kubernetes)	12	4	48	16	192	40	480	Linux	1 no- Active - Active 5 Remaining Active - Passive			
3	Mobile Server (Kubernetes)	4	16	64	64	256	60	240	Linux	Active - Active			
4	Processing Servers (Kubernetes)	4	32	128	512	2048	120	480	Linux	Active - Active			
5	Ingestion Module (Kafka)	4	8	32	64	256	520	2080	Linux	Active - Passive			
6	Databases -With High Performance SSD Block Storage with Minimum 5000 IOPS as per the Industry Standards	10	8	80	48	480	3000	30000	Linux				
7	Cache	4	8	32	16	64	120	480	Linux	Active - Passive			
8	Web Services to handle the Video data	10	8	80	32	320	40	400	Windows	Active - Passive			
9	CDN Service	1	NA	NA	NA	NA	NA	NA	NA				
10	NGFW with support for 100 endpoints	1	NA	NA	NA	NA	NA	NA	NA				
11	WAF with support for 5 Web ACL & 5 rules per ACL	1	NA	NA	NA	NA	NA	NA	NA				

Sl.	Components	Total Qty	Cores		RAM		Storage		OS	Remarks	Usage for 4 years	Unit List Price	Total List Price
		(Inclusive of HA) (X)	Core Per VM	Total Cores	RAM (GB) per VM	Total RAM (GB)	Storage for each VM (GB)	Total Storage (In GB)			(Y)	(Z)	(X*Y*Z)
12	Snapshots for the Storage Volumes for 1% daily incremental change	Daily increment considering linear increase across year	NA	NA	NA	NA	NA	NA	NA				
13	Load Balancing Server with configurable rules: Layer 4 & Layer 7	1	NA	NA	NA	NA	NA	NA	NA				
14	NAT Gateway as per the Industry Standards	1	NA	NA	NA	NA	NA	NA	NA				
15	Identity & Access Management Services	2	4	8	16	32	60	120	Linux	Active - Passive			
16	DDoS Protection Service	1	NA	NA	NA	NA	NA	NA	NA				
17	Data Transfer (Ingress)	5TB	NA	NA	NA	NA	NA	NA	NA				
18	Data Transfer (Egress)	NA	NA	NA	NA	NA	NA	NA	NA				
19	Cloud Native Network Monitoring	1	NA	NA	NA	NA	NA	NA	NA				
20	Resource Monitoring dashboards to visualize CPU, Memory, Disk utilization and alarms for threshold breach	1	NA	NA	NA	NA	NA	NA	NA				
21	24 x 7 online support via email / phone / chat	NA	NA	NA	NA	NA	NA	NA	NA				

Sl.	Components	Total Qty	Cores		RAM		Storage		OS	Remarks	Usage for 4 years	Unit List Price	Total List Price
		(Inclusive of HA) (X)	Core Per VM	Total Cores	RAM (GB) per VM	Total RAM (GB)	Storage for each VM (GB)	Total Storage (In GB)			(Y)	(Z)	(X*Y*Z)
22	Additional Storage (BLOB)- 10 TB Incremental Year wise : Year 1 : 10 TB; Additional storage will be added based on utilisation levels: Year 2 : 20 TB Year 3 : 35 TB Year 4 : 45 TB	NA	NA	NA	NA	NA	NA	NA	NA				
23	Static IP Address for the Architecture	1	NA	NA	NA	NA	NA	NA	NA				
24	VPN Connectivity to BMTC 10 P2S/VPN Users	1	NA	NA	NA	NA	NA	NA	NA				
25	DNS service with 1 million queries - 2 public, 10 private DNS zones	1	NA	NA	NA	NA	NA	NA	NA				
26	Backups as per the Industry Standards	1	NA	NA	NA	NA	NA	NA	NA				
27	Cloud Audit trail with 6 month log retention	1	NA	NA	NA	NA	NA	NA	NA				
28	Notification service	1	NA	NA	NA	NA	NA	NA	NA				
29	EDR for all VMs & Services	1	NA	NA	NA	NA	NA	NA	NA				
30	Managed API Gateway - Support 2500 requests/sec	1	NA	NA	NA	NA	NA	NA	NA				

FORM 4: MANPOWER PRICE - OPERATIONS AND MAINTENANCE PHASE

S. No	Resource Requirement for Operations & Maintenance Phase for the Cloud services (As per Annexure 1)	No. of Resources	Bid Currency	Man-Month Rate	Total Cost
1.	Cloud Infrastructure Admin	2	INR		
2.	Project Manager	1	INR		
O&M Phase Manpower Cost					**Total B**

FORM 5: RATE DISCOVERY CHART

The Service Provider shall also provide a rate card as per the template given below mentioning the on-demand price and three-year commitment price. MSP should identify all possible configuration requirements that may be needed for scaling out the infrastructure in the future. It should mention those configurations and the rates associated.

Rate Discovery Chart							
Sl.	**Components**	**Core**	**RAM (GB)**	**OS**	**Storage (GB)**		
1	VM	2	8	linux		on demand	per hr
2	VM	4	16	linux		on demand	per hr
3	VM	8	32	linux		on demand	per hr
4	VM	16	64	linux		on demand	per hr
5	VM	2	8	linux		3 year reseved	Per Month
6	VM	4	16	linux		3 year reseved	Per Month
7	VM	8	32	linux		3 year reseved	Per Month
8	VM	16	64	linux		3 year	Per Month

						reseved	
9	VM	2	8	Windows		on demand	per hr
10	VM	4	16	Windows		on demand	per hr
11	VM	8	32	Windows		on demand	per hr
12	VM	16	64	Windows		on demand	per hr
13	VM	2	8	Windows		3 year reseved	Per Month
14	VM	4	16	Windows		3 year reseved	Per Month
15	VM	8	32	Windows		3 year reseved	Per Month
16	VM	16	64	Windows		3 year reseved	Per Month
17					per GB HDD attach to Any VM		Per Month
18					per GB SSD Disk attachable to any VM with standard throughput		Per Month
19					1000 GB SSD Disk attachable to any VM with provisioned throughput IOPS of at least 5000 IOPS		Per Month
20					1000 GB Block Storage - Active/Hot Tier		Per Month
21					1000 GB Block Storage - Archival Tier		Per Month
22	16 vCPUs, VM with Windows Server + SQL Server Enterprise		64			on Demand	Per Hr
23	32 vCPUs, VM with Windows Server + SQL Server Enterprise		128			on Demand	Per Hr
24	16 vCPUs, VM with Windows Server + SQL Server Enterprise		64			3 years Reserved	Per Month
25	32 vCPUs, VM with Windows Server + SQL Server Enterprise		128			3 years Reserved	Per Month

26	Network Firewall per Firewall instance - filtering inbound & outbound with min 2.5 Gbps throughput and up to 2 TB data processed per month, up to 50 end points behind each firewall						Per Month
27	Web Application Firewall - throughput of 50 Mbps with HTTP/S support and protection of up to 100 separate application clusters/ACL						Per Month
28	Disk snapshot per TB						Per month
29	Network Load Balancer 5 rules						Per month
30	Virtual Network/ Nat Gateway within DC to create zones - per 100 GB with 1 TB outbound data transfer to edge						Per month
31	Layer 4 and 7 DDoS service per VM						Per month
32	Network Monitor - 100 GB logs per month						Per month
33	Static IP Addresses						Per month
34	VPN Gateway with 100 P2S connections,						Per month
35	DNS Services - 2 External, 100 internal						Per month
36	Data Transfer (Egress), 500GB						Per Month
37	VM backup with up to 500 GB disk						Per VM per month
38	Disk Backup per TB						Per month
39	Monitoring and observability service - No. of metrics - 100 Logs , Standard Logs - Data Ingested - 5 GB per day, Analysis Logs - Data ingested - 5 GB per day, Retention - 30 days						Per month
40	EDR/Antivirus Solution per VM						Per month

41	Managed DB as a service - PostGres 8 vCPU 3 years reserved, 100 GB Storage instance						Per Month
42	Managed DB as a service - MySQL 8 vCPU 3 years reserved, 100 GB Storage instance						Per Month
43	Managed DB as a service - SQL Server Enterprise 8 vCPU 100 GB Storage 3 years reserved instance						Per Month
44	Bastion as a service - 1 unit - 730 hrs						Per Month
45	Bandwidth - inbound per 100 GB						Per Month
46	Bandwidth - outbound per 100 GB						Per Month
47	Managed HSM service in high availability from CSP						Per Month

Commercial evaluation would be done on the section 4 of Financial Bid. Rate Discovery Chart will not be considered for Commercial Evaluation. While BMTC reserves the right to scale up or scale down any of the **components of A** as a result of optimization or may raise change request as per BMTC's business requirements. The required change requests should be processed within 24 hours by selected bidder and billing should be done on pro-rata basis on actual usage by BMTC.

Procedure for entering line items in e-procurement portal:

All the above Financial Forms are for reference purpose only to demonstrate the evaluation process. The bidders have to enter their quotation only in the method described below: The bidders must follow the steps given below to fill their financial quotation and the cost breakup for each line item as **per Form 2, Form 4 and Form 5 above.** The line items to be used for quotation have been given in the next section.

Step 1: The bidder has to login to the e-procurement portal and under the 'Financial Offer (inclusive of Statutory/Tax Costs)' tab, they must fill in the Total for 4 years i.e. (Total Price=A+B) from **Form 1 above.**

Step 2: Then, under the tab 'Provide the breakup of taxes included', click on the dropdown 'Select the component'**.**

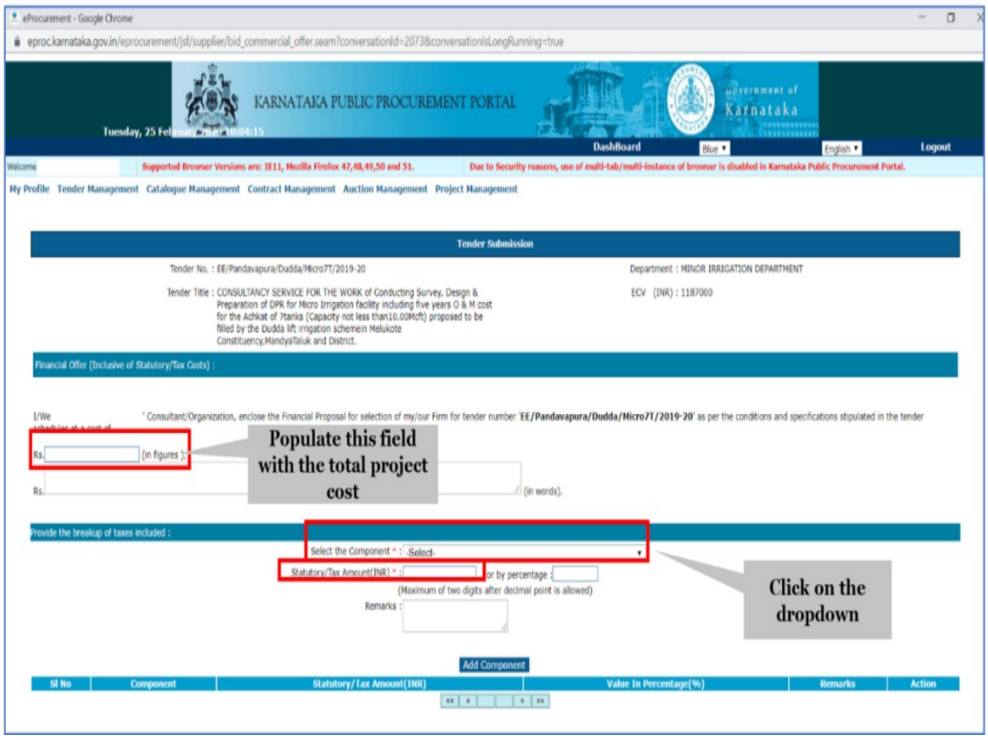
Step 3: Select 'Other Levies' from the dropdown

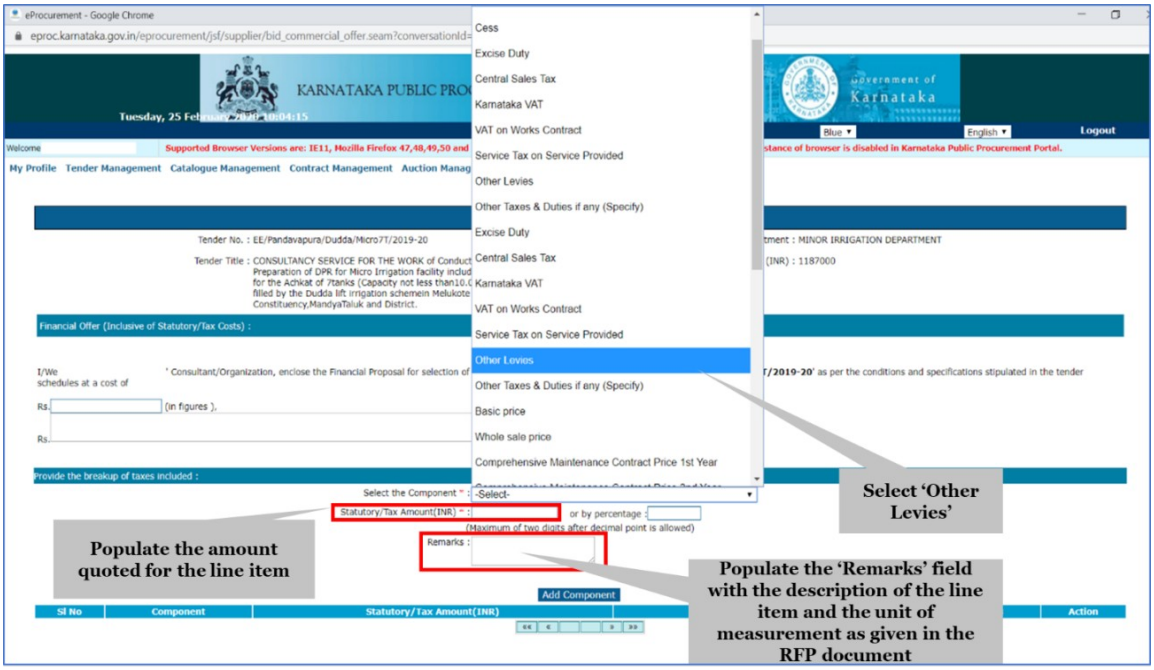
Step 4: Populate the **'Remarks'** field with the description of the line item as given in the RFP document Table 'Line Items for quotation in e-procurement portal'

Step 5: Populate the corresponding amount **as** in Forms 2, 4 and 5 above quoted for the line item in the field **'Statutory/Tax Amount'**

Step 6: Click on **'Add Component'** button to add new line items and follow steps 2 to 5 to add all the**107-line items.**

The sample screenshots for the above steps are given below:


KARNATAKA PUBLIC PROCUREMENT PORTAL
Tender Submission
Financial Offer (Inclusive of Statutory/Tax Costs) :
Populate this field with the total project cost
Provide the breakup of taxes included :
Click on the dropdown
Add Component



"Upload lump sum value in e-portal and submit breakup cost in separate sealed envelope and the same may be opened during financial bid opening".

Line Items for quotation in the e-procurement portal:

Bill of Material - Cloud Services - Reserved Instances			
Sl.	**Components**	**Total Qty (Inclusive of HA) (X)**	
1	BI Server (BOAP & Helpdesk - IMMS)	8	Usage for 4 years (Y)
2	BI Server (BOAP & Helpdesk - IMMS)	8	Unit Price(Z)
3	Web Servers (Kubernetes)	12	Usage for 4 years (Y)
4	Web Servers (Kubernetes)	12	Unit Price(Z)
5	Mobile Server (Kubernetes)	4	Usage for 4 years (Y)
6	Mobile Server (Kubernetes)	4	Unit Price(Z)
7	Processing Servers (Kubernetes)	4	Usage for 4 years (Y)
8	Processing Servers (Kubernetes)	4	Unit Price(Z)
9	Ingestion Module (Kafka)	4	Usage for 4 years (Y)
10	Ingestion Module (Kafka)	4	Unit Price(Z)
11	Databases -With High Performance SSD Block Storage with Minimum 5000 IOPS as per the Industry Standards	10	Usage for 4 years (Y)
12	Databases -With High Performance SSD Block Storage with Minimum 5000 IOPS as per the Industry Standards	10	Unit Price(Z)
13	Cache	4	Usage for 4 years (Y)
14	Cache	4	Unit Price(Z)
15	Web Services to handle the Video data	10	Usage for 4 years (Y)

16	Web Services to handle the Video data	10	Unit Price(Z)
17	CDN Service	1	Usage for 4 years (Y)
18	CDN Service	1	Unit Price(Z)
19	NGFW with support for 100 endpoints	1	Usage for 4 years (Y)
20	NGFW with support for 100 endpoints	1	Unit Price(Z)
21	WAF with support for 5 Web ACL & 5 rules per ACL	1	Usage for 4 years (Y)
22	WAF with support for 5 Web ACL & 5 rules per ACL	1	Unit Price(Z)
23	Snapshots for the Storage Volumes for 1% daily incremental change	Daily incrementconsidering linear increase across year	Usage for 4 years (Y)
24	Snapshots for the Storage Volumes for 1% daily incremental change	Daily incrementconsidering linear increase across year	Unit Price(Z)
25	Load Balancing Server with configurable rules: Layer 4 & Layer 7	1	Usage for 4 years (Y)
26	Load Balancing Server with configurable rules: Layer 4 & Layer 7	1	Unit Price(Z)
27	NAT Gateway as per the Industry Standards	1	Usage for 4 years (Y)
28	NAT Gateway as per the Industry Standards	1	Unit Price(Z)
29	Identity & Access Management Services	2	Usage for 4 years (Y)
30	Identity & Access Management Services	2	Unit Price(Z)
31	DDoS Protection Service	1	Usage for 4 years (Y)
32	DDoS Protection Service	1	Unit Price(Z)
33	Data Transfer (Ingress)	5TB	Usage for 4 years (Y)
34	Data Transfer (Ingress)	5TB	Unit Price(Z)
35	Data Transfer (Egress)	NA	Usage for 4 years (Y)
36	Data Transfer (Egress)	NA	Unit Price(Z)
37	Cloud Native Network Monitoring	1	Usage for 4 years (Y)
38	Cloud Native Network Monitoring	1	Unit Price(Z)
39	Resource Monitoring dashboards to visualize CPU, Memory, Disk utilization and alarms for threshold breach	1	Usage for 4 years (Y)
40	Resource Monitoring dashboards to visualize CPU, Memory, Disk utilization and alarms for threshold breach	1	Unit Price(Z)
41	24 x 7 online support via email / phone / chat	NA	Usage for 4 years (Y)
42	24 x 7 online support via email / phone / chat	NA	Unit Price(Z)
43	Additional Storage (BLOB)- 10 TB Incremental Year wise : Year 1 : 10 TB; Additional storage will be added based on utilisation levels: Year 2 : 20 TB Year 3 : 35 TB Year 4 : 45 TB	NA	Usage for 4 years (Y)

44	Additional Storage (BLOB)- 10 TB Incremental Year wise : Year 1 : 10 TB; Additional storage will be added based on utilisation levels: Year 2 : 20 TB Year 3 : 35 TB Year 4 : 45 TB	NA	Unit Price(Z)
45	Static IP Address for the Architecture	1	Usage for 4 years (Y)
46	Static IP Address for the Architecture	1	Unit Price(Z)
47	VPN Connectivity to BMTC 10 P2S/VPN Users	1	Usage for 4 years (Y)
48	VPN Connectivity to BMTC 10 P2S/VPN Users	1	Unit Price(Z)
49	DNS service with 1 million queries - 2 public, 10 private DNS zones	1	Usage for 4 years (Y)
50	DNS service with 1 million queries - 2 public, 10 private DNS zones	1	Unit Price(Z)
51	Backups as per the Industry Standards	1	Usage for 4 years (Y)
52	Backups as per the Industry Standards	1	Unit Price(Z)
53	Cloud Audit trail with 6 month log retention	1	Usage for 4 years (Y)
54	Cloud Audit trail with 6 month log retention	1	Unit Price(Z)
55	Notification service	1	Usage for 4 years (Y)
56	Notification service	1	Unit Price(Z)
57	EDR for all VMs & Services	1	Usage for 4 years (Y)
58	EDR for all VMs & Services	1	Unit Price(Z)
59	Managed API Gateway - Support 2500 requests/sec	1	Usage for 4 years (Y)
60	Managed API Gateway - Support 2500 requests/sec	1	Unit Price(Z)

Rate Discovery Chart			
Sl	**Cloud Service / Plan**	**Unit Rate**	**Unit Price**
61	2 vCPUs, 8 GB RAM VM with Linux on Demand	Per Hr	
62	4 vCPUs, 16 GB RAM VM with Linux on Demand	Per Hr	
63	8 vCPUs, 32 GB RAM VM with Linux on Demand	Per Hr	
64	16 vCPUs, 64 GB RAM VM with Linux on Demand	Per Hr	
65	2 vCPUs, 8 GB RAM VM with Linux 3 yr. Reserved	Per Month	
66	4 vCPUs, 16 GB RAM VM with Linux 3 yr. Reserved	Per Month	
67	8 vCPUs, 32 GB RAM VM with Linux 3 yr. Reserved	Per Month	
68	16 vCPUs, 64 GB RAM VM with Linux 3 yr. Reserved	Per Month	
69	2 vCPUs, 8 GB RAM VM with Windows on Demand	Per Hr	
70	4 vCPUs, 16 GB RAM VM with Windows on Demand	Per Hr	

71	8 vCPUs, 32 GB RAM VM with Windows on Demand	Per Hr	
72	16 vCPUs, 64 GB RAM VM with Windows on Demand	Per Hr	
73	2 vCPUs, 8 GB RAM VM with Windows 3 yr. Reserved	Per Month	
74	4 vCPUs, 16 GB RAM VM with Windows 3 yr. Reserved	Per Month	
75	8 vCPUs, 32 GB RAM VM with Windows 3 yr. Reserved	Per Month	
76	16 vCPUs, 64 GB RAM VM with Windows 3 yr. Reserved	Per Month	
77	per GB HDD attach to Any VM	Per Month	
78	per GB SSD Disk attachable to any VM with standard throughput	Per Month	
79	1000 GB SSD Disk attachable to any VM with provisioned throughput IOPS of at least 5000	Per Month	

	IOPS		
80	1000 GB Block Storage - Active/Hot Tier	Per Month	
81	1000 GB Block Storage - Archival Tier	Per Month	
82	16 vCPUs, 64 GB RAM VM with Windows Server + SQL Server Enterprise on Demand	Per Hr	
83	32 vCPUs, 128 GB RAM VM with Windows Server + SQL Server Enterprise on Demand	Per Hr	
84	16 vCPUs, 64 GB RAM VM with Windows Server + SQL Server Enterprise 3 yr. Reserved	Per Month	
85	32 vCPUs, 128 GB RAM VM with Windows Server + SQL Server Enterprise 3 yr. Reserved	Per Month	
86	Network Firewall per Firewall instance - filtering inbound & outbound	Per month	

	with min 2.5 Gbps throughput and up to 2 TB data processed per month, up to 50 end points behind each firewall		
87	Web Application Firewall - throughput of 50 Mbps with HTTP/S support and protection of up to 100 separate application clusters/ACL	Per month	
88	Disk snapshot per TB	Per month	
89	Network Load Balancer 5 rules	Per month	
90	Virtual Network/ Nat Gateway within DC to create zones - per 100 GB with 1 TB outbound data transfer to edge	Per month	
91	Layer 4 and 7 DDoS service per VM		
92	Network Monitor - 100 GB logs per	Per month	

	month		
93	Static IP Addresses		
94	VPN Gateway with 100 P2S connections,	Per month	
95	DNS Services - 2 External, 100 internal	Per month	
96	Data Transfer (egress), 500 GB	Per month	
97	VM backup with up to 500 GB disk	Per month	
98	Disk Backup per TB	Per VM per month	
99	Monitoring and observability service - No. of metrics - 100 Logs Standard Logs - Data Ingested - 5 GB per day, Analysis Logs - Data ingested - 5 GB per day, Retention - 30 days	Per month	
100	EDR/ Antivirus Solution per VM	Per month	
101	Managed DB as a service - PostGres 8 vCPU 3 yr. reserved, 100 GB Storage instance	Per month	

102	Managed DB as a service - MySQL 8 vCPU 3 yr. reserved, 100 GB Storage instance	Per Month	
103	Managed DB as a service - SQL Server Enterprise 8 vCPU 100 GB Storage 3 yr. reserved instance	Per Month	
104	Bastion as a service - 1 unit - 730 hrs.	Per Month	
105	Bandwidth - inbound per 100 GB	Per month	
106	Bandwidth - outbound per 100 GB	Per month	
107	Managed HSM service in high availability from CSP	Per month	

SECTION 5: TERMS OF REFERENCE (TOR)

1. ABOUT BMTC

The Bengaluru Metropolitan Transport Corporation is the sole public bus transport provider for Bengaluru, serving urban, sub-urban and rural areas. BMTC is committed to provide quality, safe, reliable, clean and affordable travel. The testimony of its success lies in increasing passenger trips everyday by a wide range of customer base. To modernize its services for commuter comfort, BMTC strives to strengthen information systems and improve processes through introduction of intelligent technology solution, make capacity enhancement through infrastructure development, user-friendly interchange facilities, fleet upgradation and augmentation, apart from its core activities, which includes fare structuring, route network optimization, planning and monitoring. BMTC reaches far and wide, in every nook and corner of the city, making public transport an attractive travel choice for everyone. BMTC's stronghold in the area of public transport in Bengaluru is a testimony to its adoption of sound Management, HR, Quality and Environmental policies and strong support from the Government of Karnataka and esteemed passengers.

2. ABOUT BMTC'S MOBILE APP PROJECT

BMTC has increased focus on passenger safety, especially women commuters and is on the way of bringing in improved vehicle tracking system, video surveillance, PIS boards at bus stops and analytics capability. It has decided to equip its buses with new AIS 140 compliant vehicle tracking devices which will feed data to the vehicle tracking application. The initiative also includes bringing in an advanced mobile application that can be used by Women commuters to seek remote assistance in case of emergency, tracking movements of women passengers when support is sought by them, putting on-board cameras to monitor on-bus activities, installing panic buttons within buses for women passengers to seek remote assistance in situation of emergency and creating a centralized helpline for providing assistance during distress and Passenger Information System at Bus Stops/Stations for displaying Bus Arrival Information.

Component of the project includes:

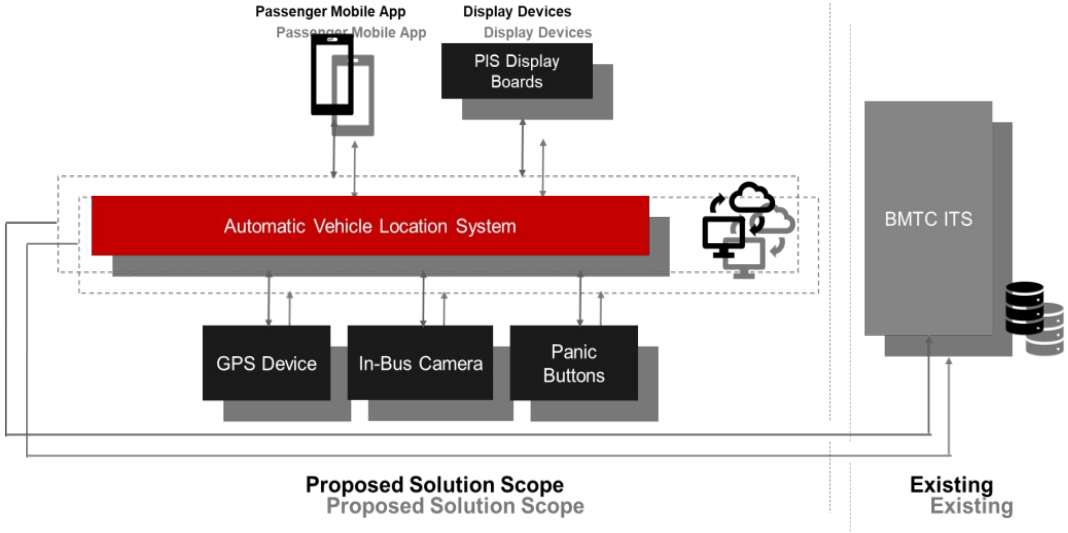
a) Mobile Application with women safety features.
b) CCTV system with Camera, Mobile network video recorder (mNVR) and Emergency buttons.
c) Automatic Vehicle Location System (AVLS)
d) Bus Operations and Analytics Platform (BOAP)
e) Passenger Information Display System

Scope of Work:

- Mobile App with Women Safety Feature.
- Emergency Response System – Panic Button.
- Automatic Vehicle Location System (AVLS) for 5000 buses.
- Bus Operations and Analytics Platform (BOAP).
- PIS Boards for display of Bus Schedule, ETA at 500 Bus Stops/Stations.

- In-bus Surveillance System for 5000 buses.
- Integration with BMTC's existing ITS.
- Data sharing platform with open protocols for sharing data with third party agencies.
- Maintenance of all installed hardware & Software.

BMTC intends to generate maximum value from the new initiatives as well as its existing ITS solution and wants to enhance BMTC's ITS infrastructure to support the requirements.



3. **BACKGROUND**

In an effort to enhance its IT infrastructure, BMTC feels the necessity to move to cloud as it envisions multiple benefits like:

- Saving on capital expenditure to be incurred for replacing End of Life infrastructure

- Leverage on-demand storage capacity
- Ensure higher uptime and system availability
- Achieve higher scalability future increase in resource requirement
- Provide flexibility in using the resources, taking backup and restoration by business users through self-service mechanism

This tender is intended to select a Managed Service Provider (MSP) who will implement and provide the cloud services to assist BMTC in its journey towards an improved and secure mobility system.

4. **SCOPE OF WORK**

As part of the **managed services that will be required to be undertaken by the MSP, a broad categorization of the scope of work is given below.**

Sl.	Activity
1	Provisioning and Setup of Cloud Services
2	Operations & Maintenance of Cloud services
3	Acceptance and Validation of Cloud Environment
4	Exit Management Plan/ Transition-Out Services and training.
5	Cloud Services Specifications and Requirements

The details of the activities to be undertaken under each of the above category are as follows:

A. PROVISIONING, SETUP OF CLOUD SERVICES, TRAINING AND KNOWLEDGE TRANSFER

a. PROVISIONING OF CLOUD SERVICES

a) The MSP shall be responsible for provisioning of required software, infrastructure, bandwidth, licenses and management of services deployment, including the underlying application/system software necessary to run the applications. MSP shall coordinate with BMTC/it's SI to adequately and optimally size the necessary compute, memory, and storage required, build the minimum sufficient redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP at all times. The hosting solution must be designed for rapid elasticity and handle instance failures without downtime.

b) The MSP needs to **carry out the capacity planning in advance**, in consultation with BMTC to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.

c) The MSP shall deploy the services on **a Virtual Private Cloud. The environment of virtual private cloud shall comply with the respective Provisional Empanelment Compliance requirements published by MeiTy, GoI.**

d) The services shall be hosted in a manner so as to **ensure high-availability of the infrastructure while maintaining the required uptime SLA. Critical services such as Database**

servers (RDBMS) shall be deployed in High-availability mode, while other services shall be configured with auto-scaling and auto-healing mode to ensure high-availability.

e) The Database nodes (RDBMS) should be in a separate subnet with higher security layer. The testing and development instances of the application should be in a separate subnet from the production instance and setup such that users of the environments are in separate networks.
f) Setup, install, configure, manage, upgrade, and migrate all components of the application including application servers, database servers and storage and the application code, with help and guidance from the application development agency.
g) Maintain and manage the required network components for the cloud service procured.
h) Be responsible for implementation, management and monitoring of tools and services used for the application like Next Generation Firewall (NGFW), Web Application Firewall (WAF), DDoS protection etc.
i) Configure external connections required to upload database/files etc.
j) Understand the complete architecture of the application and process necessary for smooth setup and migration of applications and databases including interdependencies between applications and data.
k) Responsibility of the MSP/CSP to provide cloud specialist services during implementation phase.

b. TRAINING AND KNOWLEDGE TRANSFER

- Provide training and support to engineers/professionals identified by the department, either on-site or online as and when required, on cloud management.
- Provide necessary technical documentations, design documentations, Standard Operating Procedures (SOPs) required for operations and management of cloud services.
- Provide necessary technical documentation and SOP for conducting a porting exercise from existing cloud to another cloud or on-premises data centre.
- Training to be provided to BMTC identified personnel on Monitoring Dashboard, console, SLA parameter console etc.,
- Conduct the training and knowledge transfer in the first 2 years of contract.

c. BILL OF MATERIALS FOR CLOUD SERVICES

Bill of Material - Cloud Services - Reserved Instances												
Sl.	**Components**	**Total Qty**	**Cores**		**RAM**		**Storage**		**OS**	**Remarks**	**Usage for 4 years**	**Unit List Price**	**Total List Price**
		(Inclusive of HA) (X)	**Core Per VM**	**Total Cores**	**RAM (GB) per VM**	**Total RAM (GB)**	**Storage for each VM (GB)**	**Total Storage (In GB)**			**(Y)**	**(Z)**	**(X*Y*Z)**
1	BI Server (BOAP & Helpdesk - IMMS)	8	8	64	32	256	90	720	Windows	Active - Passive			
2	Web Servers (Kubernetes)	12	4	48	16	192	40	480	Linux	1 no- Active - Active 5 Remaining Active - Passive			
3	Mobile Server (Kubernetes)	4	16	64	64	256	60	240	Linux	Active - Active			
4	Processing Servers (Kubernetes)	4	32	128	512	2048	120	480	Linux	Active - Active			
5	Ingestion Module (Kafka)	4	8	32	64	256	520	2080	Linux	Active - Passive			
6	Databases -With High Performance SSD Block Storage with Minimum 5000 IOPS as per the Industry Standards	10	8	80	48	480	3000	30000	Linux				
7	Cache	4	8	32	16	64	120	480	Linux	Active - Passive			
8	Web Services to handle the Video data	10	8	80	32	320	40	400	Windows	Active - Passive			
9	CDN Service	1	NA	NA	NA	NA	NA	NA	NA				
10	NGFW with support for 100 endpoints	1	NA	NA	NA	NA	NA	NA	NA				
11	WAF with support for 5 Web ACL & 5 rules per ACL	1	NA	NA	NA	NA	NA	NA	NA				

Sl.	Components	Total Qty	Cores		RAM		Storage		OS	Remarks	Usage for 4 years	Unit List Price	Total List Price
		(Inclusive of HA) (X)	Core Per VM	Total Cores	RAM (GB) per VM	Total RAM (GB)	Storage for each VM (GB)	Total Storage (In GB)			(Y)	(Z)	(X*Y*Z)
12	Snapshots for the Storage Volumes for 1% daily incremental change	Daily increment considering linear increase across year	NA	NA	NA	NA	NA	NA	NA				
13	Load Balancing Server with configurable rules: Layer 4 & Layer 7	1	NA	NA	NA	NA	NA	NA	NA				
14	NAT Gateway as per the Industry Standards	1	NA	NA	NA	NA	NA	NA	NA				
15	Identity & Access Management Services	2	4	8	16	32	60	120	Linux	Active - Passive			
16	DDoS Protection Service	1	NA	NA	NA	NA	NA	NA	NA				
17	Data Transfer (Ingress)	5TB	NA	NA	NA	NA	NA	NA	NA				
18	Data Transfer (Egress)	NA	NA	NA	NA	NA	NA	NA	NA				
19	Cloud Native Network Monitoring	1	NA	NA	NA	NA	NA	NA	NA				
20	Resource Monitoring dashboards to visualize CPU, Memory, Disk utilization and alarms for threshold breach	1	NA	NA	NA	NA	NA	NA	NA				
21	24 x 7 online support via email / phone / chat	NA	NA	NA	NA	NA	NA	NA	NA				

Sl.	Components	Total Qty	Cores		RAM		Storage		OS	Remarks	Usage for 4 years	Unit List Price	Total List Price
		(Inclusive of HA) (X)	Core Per VM	Total Cores	RAM (GB) per VM	Total RAM (GB)	Storage for each VM (GB)	Total Storage (In GB)			(Y)	(Z)	(X*Y*Z)
22	Additional Storage (BLOB)- 10 TB Incremental Year wise : Year 1 : 10 TB; Additional storage will be added based on utilisation levels: Year 2 : 20 TB Year 3 : 35 TB Year 4 : 45 TB	NA	NA	NA	NA	NA	NA	NA	NA				
23	Static IP Address for the Architecture	1	NA	NA	NA	NA	NA	NA	NA				
24	VPN Connectivity to BMTC 10 P2S/VPN Users	1	NA	NA	NA	NA	NA	NA	NA				
25	DNS service with 1 million queries - 2 public, 10 private DNS zones	1	NA	NA	NA	NA	NA	NA	NA				
26	Backups as per the Industry Standards	1	NA	NA	NA	NA	NA	NA	NA				
27	Cloud Audit trail with 6 month log retention	1	NA	NA	NA	NA	NA	NA	NA				
28	Notification service	1	NA	NA	NA	NA	NA	NA	NA				
29	EDR for all VMs & Services	1	NA	NA	NA	NA	NA	NA	NA				
30	Managed API Gateway - Support 2500 requests/sec	1	NA	NA	NA	NA	NA	NA	NA				

B. OPERATIONS & MAINTENANCE WITH OPTIMIZATION OF CLOUD SERVICES

a) RESOURCE MANAGEMENT

- MSP should offer cloud services from **CSP's MEITY Empanelled India Data Centre and must ensure that BMTC data resides only in India.**
- While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provided in the RFP, subsequently, it is expected that the MSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, and storage as per the performance requirements of the solution and meet the SLAs **using the auto-scaling features provided by the CSP.**
- In addition to auto-scaling, for any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.
- The scaling up/scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by the BMTC. The Service Provider shall provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth/demand and any other details justifying the request to scale up or scale down. **The Service Provider shall also provide rates in rate discovery chart as per the format mentioned in Section 4.** MSP should identify all possible configuration requirements that may be needed for scaling out the infrastructure in the future. **It should mention those configurations and the rates associated in the Section 4.**
- Be responsible for porting to another cloud or to on premises data centre as and when required by the department, with zero data loss and fully functional application as exists on existing cloud.
- Ensure and meet all standard data formats for data transfer/portability from one cloud to another or to on-premises data centre.
- Work out migration plan for non-cloud and cloud architecture during and after the migration period in close coordination with the department.
- Ensure high resiliency, hyper scalability, minimum latency etc.
- Be responsible for security of facilities, physical security of Hardware, network infrastructure, virtualisation infrastructure, and other platform services configured for the entire application, as per the shared responsibility model of MeiTy.

b) PATCH & CONFIGURATION MANAGEMENT

- Bidder shall provide managed service for system patch and

configuration management.

- Critical security patches are applied as needed, or when updates or patches are released from OS vendors.
- Bidder must ensure patch and updates applies in a timely and consistent manner to minimize the impact on business.

c) USER ADMINISTRATION

- Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.
- Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account
- Securely control users' access to Cloud services using a range of security credentials including passwords, key pairs, and X.509 certificates.
- Offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device/mechanism.
- Provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production. Support a policy validator to automatically examine non-compliant access control policies.
- Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.

d) SECURITY ADMINISTRATION

- Appropriately configure the security groups in accordance with the BMTC’s networking policies.
- Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
- Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
- Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.
- Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with BMTC’s policies.
- Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by BMTC’s policies.
- Review the audit logs to identify any unauthorized access to BMTC's systems.
- **Bidder should provide the Management console to monitor the security events, real time traffic monitoring, real time troubleshooting.**

e) BACKUP ON CLOUD

- Configure, schedule, monitor and manage backups of all the data

including but not limited to files, images and databases as per the policy finalized by BMTC. BMTC/its SI may randomly cross check the backed-up databases on a weekly basis to ensure the integrity of the backup operations.

- Restore from the backup where required.
- Provide full backup to BMTC in their local storage during the end of contract or as and when requested by BMTC.

f) MONITORING PERFORMANCE AND SERVICE LEVELS

- **Provide and implement tools and processes for monitoring the availability of assigned applications, measuring the service levels, application/Severs/Storage/Network performance and utilization responding to system outages with troubleshooting activities designed to identify and mitigate operational issues**. **The tool shall be capable of providing the exact utilization of servers and shall be able to generate per day, per month and per quarter utilization reports based on which the payments will be made to the Bidder.**
- Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels.
- Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g., for triggering elasticity, request rates, number of users connected to a service.
- Detecting and reporting service level agreement infringements.
- Monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications including API access within the cloud service provider’s boundary.
- Monitoring the uptime of the applications hosted on the cloud and reports any deviation to the application SI/BMTC.

g) USAGE REPORTING AND BILLING MANAGEMENT

- Track system usage and usage reports.
- Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects.
- Provide the relevant reports including real time as well as past data/information/reports for BMTC to validate the billing and SLA related penalties.

h) SUPPORT FOR THIRD PARTY AUDITS AND COMPLIANCE

- Enable the logs and monitoring as required to support for third party audits
- Enable third party vulnerability assessment and penetration testing as on when required.
- Audit: Capability to provide and record logs of all user activity within a cloud environment including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the

response elements returned by the Cloud service. The API activity history should be delivered within a reasonable timeframe (<30 minutes) from the time API call is made. Capability to support storing log files in a durable and inexpensive storage solution.

- Network logs: Capability to capture information about the IP traffic going to and from network interfaces in your Private Cloud that can be used to troubleshoot why specific traffic is not reaching an instance, or as a security tool to monitor the traffic that is reaching your instance.
- Governance and Compliance: Capability to discover all of cloud resources and view the configuration of each. Continuously monitor and record your Cloud resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. Receive notifications each time a configuration changes, as well as dig into the configuration history to perform incident analysis. Capability to obtain details of what a resource's configuration looked like at any point in the past. Capability to notify every configuration change so customers can process these notifications programmatically.

i) INFRASTRUCTURE EVENT MANAGEMENT

MSP shall lead a highly focused engagement to provide BMTC you with architectural and operational guidance, as well as real-time support for your planned important events.

- MSP shall interact with BMTC and understand the success criteria and desired outcome of the event.
- Assess the readiness of the cloud environment, help identify and mitigate risks, and document the plan.
- Execute your event in coordination with BMTC to meet the desired outcome.
- Analyse results post-event and scale services to normal operating levels.

j) MISCELLANEOUS

- Advise BMTC on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
- Interface with the Cloud Service Provider(s) on behalf of BMTC for all activities including monitoring the reports (e.g., usage, security, SLA,), raising (or escalating) tickets / incidents and tracking the same to resolution.
- Prepare a comprehensive O&M plan for managing the cloud services and keep it updated with any changes during the course of the project.
- Create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.

C. ACCEPTANCE AND VALIDATION OF CLOUD ENVIRONMENT

a. ACCEPTANCE TEST

a) Test of the cloud shall be completed by the MSP and results of the same shall be shared with BMTC as specified in the accepted solution design by BMTC/its SI.

b) The User Acceptance Tests (and repeats of such tests) shall be conducted by BMTC/it's SI in coordination with the MSP during Commissioning of the Cloud Infrastructure, to ascertain whether the Cloud Infrastructure conforms to the Technical Requirements and meets the BMTC's performance requirements, including, but not restricted to, the functional and technical performance requirements. **The User Acceptance Tests shall be conducted in accordance with the test scripts provided by the MSP and approved by BMTC/its SI.**

c) BMTC shall issue a User Acceptance Certificate after successful completion of UAT. BMTC shall also notify the MSP in writing of any defect for deficiencies or other reason for the failure of the UAT, if any. The MSP shall use all reasonable endeavours to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the User Acceptance Test that the BMTC has notified the MSP. Once the MSP has made such remedies, it shall notify BMTC, and BMTC, with full cooperation of the MSP, shall use all reasonable endeavours to promptly carry out retesting of the System. Upon the successful conclusion of the User Acceptance Tests including successfully complying all integration touch points, BMTC shall issue the User Acceptance Certification.

b. STABILIZATION PHASE

a) Stabilization Period of 60 days will start after the UAT of the Cloud is over.

b) The MSP shall support BMTC/its SI in monitoring the Cloud Infrastructure for the stabilization period of 60 days after the Successful UAT.

c. GO-LIVE

After successful completion of stabilization activities, the system will be declared Go-Live. The Incident/issue free period of 60 days after the UAT shall be treated as a primary criterion for Go-Live of the project as per the SLA requirements. The MSP in coordination with BMTC should finalize additional Go-Live criteria if any.

Note:

i. Bidder has to factor the cost of provisioning of the infrastructure, database instances, and any other services required to accept/validate the cloud environments.

ii. Any licenses required for such acceptance/validation is the responsibility of the bidder.

D. EXIT MANAGEMENT PLAN / TRANSITION-OUT SERVICES

The MSP would be required to complete following activities: -

a) This Exit Management plan shall be furnished in writing to the

Purchaser or its nominated agencies at least 180days before expiry of the contract.

b) Create the environment in client identified data centre and migrate all applications with data.

c) Retain the data at the end of the agreement (for a maximum of 60 days beyond the expiry of the Agreement).

d) Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of the user departments of BMTC.

e) Support and assist BMTC, for a period of 2 months to successfully deploy and access the services from the new environment.

f) Train and transfer the knowledge to the Replacement Agency (or BMTC) to ensure similar continuity and performance of the Services post expiry of the Agreement.

g) The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with BMTC.

E. CLOUD SERVICES SPECIFICATIONS AND REQUIREMENTS

a. COMPUTE

S. No	Requirement	Description
	Compute instances – □ General Purpose □ Memory optimized □ Compute optimized □ Storage optimized □ GPU instances	Cloud provider should offer the following instance types – □ General Purpose–optimized for generic applications and provides a balance of compute, memory, and network resources. □ Memory optimized – optimized for memory applications □ Compute optimized–optimized for compute applications □ Storage optimized–include every fast/large amount of local storage for No SQL Databases and Hadoop □ GPU – intended for graphics and general-purpose GPU compute applications
	Compute instances – Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
	Compute instances – Dedicated	Cloud provider should be able offer instances that run on hardware dedicated to a single customer.
	OS Support – Linux	Cloud provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS, and Debian)
	OS Support – Windows	Cloud provider should be able to support the last two major Windows Server versions (WindowsServer2012, Windows Server 2008)
	Resize virtual cores, memory,	Resize virtual cores, memory, and storage seamlessly.

	storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and with minimal downtime
Local disk/Instance store	Cloud	service should support local storage for compute instances to be used for temporary storage of information that changes frequently.
Provision multiple concurrent instances	Cloud	service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
Instance affinity logical grouping of instances within single data centre	- Customer	should be able to logically group instances together for applications that require low network latency and/or high network throughput.
Instance anti-affinity -two or more instances hosted in different data centres		The deployment should happen in HA (High availability) so that there is no single point of failure.
Auto Scaling support	Cloud	service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.
Bring your own image/Instance Import	Customer	should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.
Export Instance Image	Cloud	service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.
Instance maintenance mitigation	Cloud	service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance.
Instance failure recovery	Cloud	service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.
Instance restart flexibility	Cloud	provider must be able to schedule events for customer's instances such as a reboot, stop/start or retirement. Depending on the event, customer might be able to act to control the timing of the event.
Support for containers	Cloud	service should support containers, including Docker and/or other containerization

		platforms.
Highly scalable, high-performance container management service	Cloud provider should offer a highly scalable, high performance container management service.	
Event-driven computing that runs code in response to events	Cloud service should be able to run customer code in response to events and automatically manage the compute resources.	
License portability and support–Microsoft	Cloud provider should offer license portability and support for Microsoft apps like SQL Server and SharePoint Server.	
License portability and support–SAP	Cloud provider should offer license portability and support for SAP apps like HANA.	
License portability and support–IBM	Cloud provider should offer license portability and support for RHEL and SUSE Linux.	
Pay-as-you-go pricing	Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity with no long- term commitments.	

b. NETWORKING

S. No.	Requirement	Description
	Multiple network interface/instance	Cloud service should be able to support multiple (primary and additional) network interfaces.
	Multiple IP addresses/instance	Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network Interface.
	Network traffic logging - Log traffic flows at network interfaces	Cloud service should support capturing information about the IP traffic going to and from network interfaces.
	Auto-assigned public IP addresses	Cloud service should be able to automatically assign a public IP to the instances.
	IP Protocol support	Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.
	Use any network CIDR, including RFC 1918	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
	Static public IP addresses	Cloud provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.

Auto-created default virtual private network	Cloud	service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address.
Subnets within private network	Customer	should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.
Subnet level filtering (Network ACLs)	Cloud	service should support subnet level filtering – Network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.
Ingress filtering	Cloud	service should support adding or removing rules applicable to inbound traffic (ingress) to instances.
Egress filtering	Cloud	service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.
Disable source/destination checks on interfaces	Cloud	service should support the ability to disable Source/destination check on network interfaces. By default, compute instances perform source/destination checks.
Configure proxy server (NAT instance) at network level	Cloud	service should support NAT instances that can route traffic from internal-only instances to the Internet.
Site-to-site managed VPN service	Cloud	service should support a hardware-based VPN connection between the cloud provider and customer data centre.
Virtual Network Peering	Cloud	service should support connecting two virtual networks to route traffic between them using private IP addresses.
Multiple VPN Connections per Virtual Network	Cloud	service should support creating multiple VPN connections per virtual network
BGP for high availability and reliable failover	Cloud	provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IP sec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.
Private connection to customer data centres	Cloud	provider should support direct leased-line connections between cloud provider and a customer data centre, office, or co-location environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. It can be implemented in future if required.
DNS based global load balancing	Cloud	service should support Load balancing of instances across multiple host servers.

Load balancing supports multiple routing methods	Cloud	service should support multiple routing mechanism including round-robin, failover, sticky session etc.
Front-end Load Balancer	Cloud	service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
Back-end Load Balancer	Cloud	service should support an internal load balancer that routes traffic to instances within private subnets.
Health checks monitor the health and performance of application	Cloud	service should support health checks to monitor the health and performance of resources.
Low Latency	The CSP	should be able to provide 10GB network connectivity between the servers if required.

c. STORAGE-BLOCK STORAGE

S. No.	Requirement	Description
	Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
	Storage volumes ≥ 1 TB	Cloud provider should offer block storage volumes greater than1 TB in size.
	SSD backed storage media	Cloud service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.
	Provisioned I/O support	Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
	Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O and snapshots using industry standard AES-256 cryptographic algorithm.
	Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
	Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
	Ability to easily share snapshots globally	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion.
	Attach more than one compute	Cloud service should support adding more than one compute instance to a single storage

	instance to a single volume	volume in R/W mode so that many users can access and share a common data source.
Consistent Input Output per second (IOPS)	Cloud	service should support a baseline IOPS/GB and maintain it consistently at scale
Annual Failure Rates <1%	Cloud	service should be durable and support annual failure rates of less than 1%

d. STORAGE – OBJECT STORAGE

S. No	Requirement	Description
	Scalable object storage service	Cloud provider should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web.
	Low-cost archival storage with policy support	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.
	Support for Server-side Encryption	Cloud service should support encryption for data at rest using256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.
	Support for Server-Side Encryption with customer – provided Keys	Cloud service should support encryption using a Key Management Service/HSM as a service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly
	Support for Server-Side Encryption with a Key Management Service	Cloud service should support encryption using a Key Management Service/HSM as a service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly
	Object lifecycle management	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion.
	Data Locality	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.
	Object change notification	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).
	High-scale static web site hosting	Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS and Java Script) and does not require server-side technologies (suchasPHPandASP.NET).
	Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in

		one bucket. Versioning protects against unintended overwrites and deletions.
Flexible access-control mechanisms		Cloud service should support flexible access-control policies to manage permissions for objects.
Audit logs		Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.
Lower Durability offering		Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.
Parallel, multipart upload		Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.
CDN option for users		Cloud provider should offer a service to speed up distribution of static and dynamic web content.
Strong Consistency		Cloud service should support read-after-write consistency for PUT operations for new objects.
Accept large data loads		Cloud provider should provide a service for moving large amounts of data into the cloud by bypassing the internet.
Deliver large data exports through shipped physical media		Deliver large data exports through cloud service

e. MANAGED RELATIONAL DATABASE AS A SERVICE

S. No.	Requirement	Description
	Managed relational database service	Cloud provider should offer a service that makes it easy to setup, operate, and scale a relational database in the cloud.
	Support for My SQL	Cloud service should support the last two major releases of My SQL (versions 5.6, 5.5) as a database engine.
	Support for Microsoft SQL Server	Cloud service should support all the editions (Express, Web, Standard, Enterprise) of SQL Server 2014 or above as a database engine.
	Support for Postgre SQL	Cloud service should support the last two major releases of Postgre SQL (9.4.x, 9.3.xor latest)
	Low latency, synchronous replication across multiple data centres in a region	The deployment should happen in HA (High availability) so that there is no single point of failure.

Read Replica support	Cloud service should support read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.
Provisioned IOPS support	Cloud service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
Bring your own SQL, Oracle licenses	Cloud service should support customers who prefer to use their existing Oracle and SQL Server database licenses in the cloud.
High Availability	Cloud Service should support enhanced availability and Durability for database instances for production workloads.
Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.
Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.
Backup	Support automated database backups

f. NON-RELATIONAL DATABASE

S. No.	Requirement	Description
	Scalable, fast and flexible No SQL database service	Cloud provider should offer a fast and flexible No SQL database service for applications that need consistent, single-digit millisecond latency at any scale.
	Replication	Cloud service should support automatic replication of data across multiple physical data centres in a region to provide high availability and data durability.
	Performance/ Latency	Cloud service should support single-digit milliseconds (TP99) latencies at any scale.
	Key-value Data Model support	Cloud service should support key value data structure where the primary key is the only required attribute for items in a table and uniquely identifies each item.
	Tenable scaling	Cloud service should support seamless throughput and storage scaling.
	Secondary Indexes	Cloud service should support secondary indexes.

		Secondary indexes are indexes that contain hash or hash-and-range keys that can be different from the keys in the table on which the index is based.
Streams	Cloud	service should support streams. Stream is an ordered flow of information about changes to items.
Database triggers	Cloud	Service should support database triggers - pieces of code that quickly and automatically respond to data modification in the tables.
Strong consistency, atomic counters	Cloud	service should support strong consistency for read operations to make sure users are always reading the latest values.
Integrated Monitoring	Cloud	service should support monitoring of request throughput and latency for database tables, among other metrics.
Integration with data warehouse	Cloud	service should support integration with a data warehouse for advanced business intelligence capabilities.
Hadoop Integration	Cloud	service should support integration with a Hadoop framework to perform complex analytics on large datasets.

SECURITY AND ADMINISTRATION

S. No.	Requirement	Description
	Control access to your cloud resources at a granular level	Cloud provider should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.
2.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
	Identify when an access key was last used to rotate old keys and remove inactive users	Cloud service should support reporting a user's access keys last use details.
	Policy Simulator to test policies before committing to production	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.
	Policy validation to ensure policies match intentions	Cloud service should support a policy validator to automatically examine non-compliant access control policies.
	Directory as a service	Cloud provider should support setting up a stand-alone directory in the cloud or connecting cloud resources with existing on- premises Microsoft Active

		Directory.
User and Group management	Cloud	service should support features such as user and group management.
Integration with your existing on-premises Active Directory	Cloud	service should integrate with existing on-premise Active Directory.
Self-service password reset for cloud users	Cloud	service should allow users to reset their password in a self-service manner.
Dedicated, hardware security module (HSM) appliance	Cloud	provider should offer dedicated HSM modules. A hardware security module (HSM) is a hardware appliance that provides secure key storage and cryptographic operations within a tamper-resistant hardware module.
Web service to record API calls and deliver log files	Cloud	provider should offer a service to record history of API calls and related events for a user account.
Receive notification of API activity	Cloud	service should support notifications when new log files are available.
Durable and inexpensive log file storage	Cloud	service should support storing log files in a durable and inexpensive storage solution.
Latency to deliver API activity history to a storage bucket	Cloud	service should deliver API activity history within a Reasonable timeframe (<30minutes) from the time API call is made.
Aggregation across multiple accounts and multiple Regions for ease of use	Cloud	service should support receiving log files from multiple regions and accounts to a single location for ease of use.
Managed service for resource inventory, configuration history & change notifications	Cloud	provider should offer a service that provides resource inventory, configuration history, and configuration change notifications to enable security and governance.
Automatically records a resource's configuration when it changes	Cloud	service should automatically record a resource Configuration when it changes and makes this information available.
Examine the configuration of your resources at any single point in the past	Customer	should be able to obtain details of what a resource's configuration looked like at any point in the past using this cloud service.
Receive notification of a configuration change	Cloud	service should notify every configuration change so customers can analyse/process these notifications

g. DEPLOYMENT AND MANAGEMENT

S. No.	Requirement	Description
1.	Service to quickly deploy and manage applications in the cloud	Cloud provider should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto- scaling to application health monitoring.
2.	Supported Platforms	Cloud service should support a wide variety of platforms from
	□Java	
	□Ruby	
	□PHP	
	□Node.js	
	□GoogleGo	
	□.NET	
	□Python	
3.	Supported OS	Cloud Service should support Windows, Linux, and Docker containers
	□Windows	
	□Linux	
	□any OS in Docker	
4.	Deployment Mechanism	Cloud service should support various deployment mechanisms, including a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio.
	□Git	
	□Zip	
	□Eclipse	
	□Visual Studio	
	□CI/CD tools	
5.	Support for SSL connections	Cloud service should support SSL connections.
6.	Application source versioning	Cloud service should support application source versioning. This would be useful for applications that have been updated and need to be redeployed.
7.	Auto scaling	Cloud service should support automatically launching or terminating instances based on the parameters such as CPU utilization defined by users.
8.	Swap virtual IP between staging and production environments	Cloud service should support swapping IP addresses between staging and production environments so that a new application version can be deployed with zero

		downtime.
9.	Integration with caching solution	Cloud service should be integrated with a caching solution such as Redis cache.
10.	Service to create a collection of related resources and provision them using a template	Cloud provider should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template.
11.	Single JSON based template to declare your stack (Desired function and not mandatory)	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application. The resources in the template should be managed as a single unit.
12.	Allow parameterization and specific configurations	Cloud service should support parameterization for specific configuration.
13.	Integration with the portal	Cloud service should be integrated with the portal.

h. APPLICATION SERVICES

S. No.	Requirement	Description
	Queuing service	Cloud provider should offer a fast, reliable, scalable, fully Managed message queuing service.
	Notification service	Cloud provider should offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
	Bulk email delivery service	Cloud provider should offer a cost-effective outbound-only email-sending service.

i. HYBRID INTEGRATION

S. No.	Requirement	Description
1.	Hardware-based virtual private networking connection to cloud resources	Cloud provider should be able to extend customer's data centre to the cloud and enable communication with their own network over an IP sec VPN tunnel.
2.	High speed, low latency, dedicated connectivity between on-premises & cloud	Cloud provider should provide mechanisms to establish private connectivity between the cloud environment and a customer data centre, office, or collocation environment.
3.	Automated VM import functionality	Cloud provider should allow customers to import VMs from a virtualization environment such as Citrix Xen, Microsoft Hyper-V,or VMware vSphere.
4.	Automated VM export functionality	Cloud provider should allow customers to export instances to their on-premises virtualization environments.
5.	Integrate with on-premises	Cloud service should integrate with existing

	Active Directory	on-premise Active Directory.
6.	Use any IP address range,	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
7.	Highly durable, automatic data replication, and recovery service from on-premises	Cloud provider should offer a service to automatically replicate data from on-premises to cloud for disaster recovery purposes.
8.	Backup service to back up on-premises servers	Cloud provider should offer a service with ability to take regular and scheduled back of on-premises servers.
9.	Utilize multi-factor authentication when accessing cloud resources	Cloud service should support multi-factor authentication. MFA requires users to prove physical possession of a hardware or virtual MFA device by providing a valid MFA code.
10.	Support from 3rd party management and monitoring tools	Cloud provider should offer management and monitoring plug-in for management solutions from multiple vendors.
11.	App. management service to deploy and operate apps in the Cloud or own data centre	Cloud provider should offer a service to automate operational tasks like software configurations, package installations, and database setups for servers running in the cloud.
12.	Service to automate code deployments to cloud and on-premises	Cloud provider should offer a service that automates code deployments to servers running in the cloud.

j. OTHER TECHNICAL REQUIREMENTS

S. No.	Requirement	Description
1.	Financial analysis recommendation engine	Cloud Service Providers must offer a service/report with minimal manual operation by which recommendations are made to the customer about configurations the customer can make to optimize their financial spend with the provider. The service must provider customer-specific recommendations based on current or historical patterns at the provider and must not be customer-generic. Recommendations must be actionable, tied to specific assets and documented as having a certain amount of financial savings. This service must be offered directly by the provider and not require the customer to seek third-party partners.
2.	Hadoop as a service	Cloud Service Providers must offer a Hadoop environment that is provided for the customer as a fully automated self-service turnkey offering. This must be a full service, not

		simply a "one click install" of Hadoop or the like.
33	Container as a Service	Cloud service provider must offer a service that allows software developers to upload, organize, run, scale, and manage containers by using container-based virtualization.
34	Content delivery network	Cloud Service Provider must offer a service for global content delivery networking. The CDN service must be offered in self-service fashion with all maintenance offered by the provider.
35	Relational DBaaS	Cloud Service provider must offer a relational database as a service (DBaaS), provided as a fully automated, self-service turnkey offering. In this service, the customer should not have access to the underlying instance, and the database maintenance must be done entirely by the provider. At a minimum, the service must support two open-source database (either MySQL or Postgre SQL) and two enterprise databases (either Microsoft SQL Server or Oracle). CSP must offer relational DB as in a locally redundant fashion, meaning that the customer database is automatically replicated across multiple data centres within a single geography.
36	SIEM integration or service	Cloud Service Providers must offer Hadoop File System out-of-the-box integration with leading SIEM products or provide a self-service, turnkey offering by which customers can configure real-time analysis and alerting of security events. At a minimum, the integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.
37	Local identity management and granular role-based authorization — network	Cloud Service Providers must include, at minimum, a local identity management system (that is, local accounts) with granular role-based authorization for network services in both the service interfaces and management console. At a minimum, the role-based authorization must support assigning authorization based on individual users and groups of users and delineation must be assignable per firewall, load balancer, IP address and network segment and support, as applicable, the following granular actions: create, delete and configure.
38	Customer VPN connectivity	Cloud Service Providers must allow customers to access the cloud service via an IP sec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This must be

		a self-service capability from the provider side, although customers will have to make configurations on their end.
9	Bulk data import/export with encryption	The provider must provide a service for bulk data import/export. Customer must be able to encrypt the data prior to transport and then decrypt it upon arrival.
10	Instance-encrypted volumes	CSP must provide an option to the customer to encrypt the data on the instance block storage volume so that data remains encrypted at rest.
11	Provider-enabled encryption services	The block and object storage services must offer customers the self-service ability from management console/Command Line Interface

k. SUPPORT

S. No.	Requirement	Description
1	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-the- minute information on service availability across multiple regions.
2	365-day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.
3	Service to compare resource usage to best practices	Cloud provider should offer a service act like a customized cloud expert and helps provision resources by following best practices.
4	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.
5	Governance and Compliance	Able to define guidelines for provisioning and configuring cloud and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources.
6	Audit Trail	Provide Audit Trail of the account activity to enable security analysis & resource change tracking.

5. **ELIGIBILITY CRITERIA**

The bidder(s) who satisfy the following qualification criteria shall be eligible to participate in the bid process. Offers received from the bidder(s) who do not fulfil all or any of the following qualification criteria are liable to be rejected.

Pre-Qualification / Eligibility Criteria:

Sl. No	Head	Eligibility Criteria	Supporting Documents
1	Company Profile	The Bidder, as a single legal entity, must be registered in India and should have been in operations in India for a minimum of three (3) years by the date of opening of the bid.	Certificates of incorporation / Registration Certificates along with Bylaws/MoA&AoA or similar legal document.
2a	Company Financials & Profile- MSP	Bidder must have minimum average turnover of INR 30 Crores for the last three (3) Financial Years (2019-20, 2020-21 and 2021-22).	Audited financial statements for last three Financial Years along with CA certificate clearly specifying turnover.
2b	Company Financials & Profile- CSP	Bidder must propose CSP who should have annual turnover of more than 300 Crores, for any three (3) financial years, out of last five (5) years for cloud business in India (2017-18, 2018-19, 2019-20, 2020-21, 2021-22)	Audited financial statements along with CA certificate clearly specifying turnover.
3	CSP Authorization	Bidder needs to be authorized by the proposed CSP to participate in the bid and shall provide the services only from that CSP under this bid.	Letter of support/ Authorization Letter from the CSP to the Bidder for providing services for this particular Project.
4	Project Experience	Bidder should have executed at least two cloud related projects each of INR 2 Crores or higher from a State/Central/PSU/private Departments/ firms in	Copy of Client certificate, work order, completion certificate or extract from the contract mentioning the scope of work.

		India.	
5a	CSP Empanelment	Bidder must propose CSP which is STQC audited and MEITY empanelled	Letter of Empanelment issued by MEITY
5b	CSP requirement	Bidder must propose CSP who must be able to provide IAAS, PAAS and SAAS as and when required by the department	Self-declaration of CSP/Copy of certificates
5c	CSP requirement	Bidder must propose CSP who should have data centres in India as per MeiTy Guidelines	Self-declaration of CSP.
6	CSP additional Security Accreditations	Bidder must propose CSP which has the following third-party certifications: ● SOC1, SOC2 ● PCI DSS Level 1 ● ISO 27017 ● ISO 27018 ● ISO 20000 ● ISO 27001 ISO Certificates for 'Business Continuity and Resilience' and 'Privacy Management (PII)': ISO 22301 and ISO 27701	Self-certificate issued on the CSP letterhead and relevant copy of the certificate.
7	No Blacklisting	The bidder should not have been blacklisted by any Central / State Government Department / PSU in India as on the bid submission date.	Self-declaration by the bidder duly notarized and signed by the authorized signatory on Non – judicial stamp paper of INR 100/-
8	No Bankruptcy / insolvency	The bidder should not have been declared bankrupt or in the process of insolvency proceedings.	Self-declaration by the Bidder duly notarized and signed by the authorized signatory on Non – judicial stamp paper of INR 100/-
9	Capability	CSP must have an Underlying Hypervisor Capability which can support 1:1 or 1:2 Physical Core to Virtual	Documents/Certificates/ Endorsement from the Cloud Provider with public link on CSP website.

		Core Ratio	
10	CSP- Public Facing Website for cloud services	CSP shall have published on its public facing website- cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across datacentre and outage details (if any) with Root Cause Analysis (RCA)	Self-Certificate issued on the CSP letterhead along with supporting document of public facing website regarding cloud services rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across data centre and outage details (if any) with Root Cause Analysis (RCA)
11	CSP- Market place solutions	Cloud Service Provider should offer Market Place solutions with first and 3rd party products and services to be used as services on their cloud platform	Self-Certificate issued on the CSP letterhead along with supporting document of having market place solutions with first and 3rd party products and services to be used as services on their cloud platform

- ✓ Bid has to be submitted by MSP only with due authorization from respective CSP.
- ✓ CSP can also bid as MSP if it meets the qualifying requirements.
- ✓ Multiple bidders can propose same CSP and a single Bidder cannot propose multiple CSP.
- ✓ **MSP should not change the proposed CSP, after bid has been submitted.**
- ✓ The bidders shall not have a conflict to interest that affects the Bidding Process. Any Bidder found to have conflict of interest shall be disqualified. A Bidder shall be deemed to have a conflict of interest affecting Bidding Process if a constituent of one Bidder is also a constituent of another Bidder.
- ✓ The Bidder (MSP) shall be responsible for meeting all obligations of the contract and the, delivery of products and services mentioned in this RFP. The Bidder (MSP) would also be responsible for ensuring the successful execution of proposed solution including meeting the SLAs.

Documents Comprising Bid Proposal:

The response submitted by the bidder shall comprise the following documents:

1. Bid Processing fee and Earnest money deposit / Bid security Declaration Form.
2. Bid Proposal form
3. General Information

4. Financial Capability with supporting documents
5. Relevant Experience with supporting documents
6. Self-Declaration
7. All relevant Certifications
8. Proposal document containing a brief about the organization, its expertise and documentary evidences.
9. Technical Proposal document

6. SERVICE LEVEL AGREEMENT

6.1. MEASUREMENT AND MONITORING

a) The SLA parameters shall be monitored **on monthly basis** as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of BMTC or an agency designated by them, then BMTC will **have the right to take services from another bidder and terminate the contract.**

b) The full set of service level reports should be available to BMTC **on a monthly basis** or based on the project requirements.

c) The Monitoring Tools shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The selected bidder shall make available the Monitoring tools for measuring and monitoring the SLAs. The bidder may deploy additional tools and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. The tools should generate the SLA Monitoring report in the end of every month which is to be shared with BMTC on a monthly basis. BMTC or its nominated agency shall have full access to the Monitoring Tools/portal (and any other tools/solutions deployed for SLA measurement and monitoring) to extract data (raw, intermediate as well as reports) as required during the project.

d) The measurement methodology/criteria/logic will be reviewed by BMTC.

e) In case of default on any of the service level metric, the selected bidder shall submit performance improvement plan along with the root cause analysis for BMTC approval.

6.2. PERIODIC REVIEWS

a) During the contract period, it is envisaged that there could be changes to the SLA, in terms of measurement methodology/logic/criteria, addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e., BMTC and selected bidder.

b) BMTC and MSP shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except by the prior written agreement of BMTC and MSP.

6.3. PENALTIES

Payments to the MSP to be linked to the compliance with the SLA metrics laid down in the agreement.

a) The payment will be linked to the compliance with the SLA

metrics.

b) The penalty in percentage of the monthly Payment is indicated against each SLA parameter in the table.

c) In case multiple SLA violations occur due to the same root cause or **incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties** for the applicable SLA violations. For example, due to a power outage there is downtime as well as some delay occurs in commissioning/delivering some committed service beyond agreed timelines because of the same outage. This means there are two SLA violations because of the same root cause (outage). Hence, whichever penalty is higher (either for service delivery failure or Downtime) will only be considered instead of adding the two penalties together.

d) The total amount of penalties levied at any month would not exceed 10% of the monthly payable amount for that month.

e) The quality of services provided by the MSP would be considered to **have reached 'Overall Critical Breach Level', if the total penalty applicable in a month reaches 20% of monthly amount.**

f) **The state of 'Overall Critical Breach' for four consecutive months will be considered as material default in providing services thus constituting a 'Material Breach'.** In case of a material breach, the MSP will be given a cure period of one month to rectify the breach failing which another one-month notice to terminate may be issued by BMTC and BMTC reserves the right to terminate the contract.

6.4. SERVICE LEVELS

Service Level Objective	Measurement and Methodology	Performance Requirements	Penalty
Pre-Go-Live			
Provisioning of cloud services		Within 30 days of issuing of LoI	The charges incurred since the launch of instances will be paid on actual usage basis. The MSP shall provide the services free of cost in lieu of the period delayed beyond 30 days
Stabilization Phase			
Stabilization Phase		Within 60 days of start of Stabilization Phase	If the stabilization phase stretches beyond 60 days, the Maintenance Phase SLAs will be applicable and corresponding penalties may be levied.
Maintenance Phase (Post Stabilization Phase)			
Uptime Availability	Availability will be measured for each of the underlying components (e.g., VM, Storage, OS, LB, Security Components) provisioned in the cloud. Measured with the help of: a. SLA reports provided by CSP b. Incident Reports from Incident	**Baseline Performance:** a) For Database Servers: **>= 99.99 % to 100 % uptime** b) For all other components of the cloud infrastructure apart from Database Server (such as application server, web server, storage, networking, firewall, etc.): **>=99.5 % to 100 % uptime**	No penalty
		Lower Performance: b) For Database Servers: **>=99 % and < 99.99 %**	5% of monthly payment

	Management Reporting system. Uptime availability shall be calculated on a monthly basis	c) For all other components of the cloud infrastructure apart from Database Server (such as application server, web server, storage, networking, firewall, etc.): **>=98 % and < 99.5 %**	
		Breach: a) For Database Servers:**< 99 %** b) For all other components of the cloud infrastructure apart from Database Server (such as application server, web server, storage, networking, firewall, etc.):**< 98%**	10 % of monthly payment
Security breach including Data Theft/Loss/ Corruption	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes Incidents pertaining to CSPs only).	No breach	For each breach/data theft, penalty will be levied as per following Criteria. 1. Severity 1 (as defined below under Note Sl no. 6 - Penalty of Rs 15 Lakhs per incident. 2. Severity 2 (as defined below under Note Sl no. 6) Penalty of Rs 10 Lakhs per incident. 3. Severity 3 (as defined below under Note Sl no. 6) Penalty of Rs 5 Lakhs per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security

			wherein the data is stolen or corrupted, BMTC reserves the right to terminate the contract.
Alert generation	Difference between the email trigger time and the Time of Lower Performance/Breach occurrence from Incident Management Reporting system	Alert should be sent to configured email IDs in the case of 'Lower Performance' and 'Breach' conditions for 'Uptime Availability'. Baseline Performance: • Alert sent **within 1 minute** of 'Lower Performance'/'Breach' conditions of 'Uptime Availability'	No Penalty
		Lower Performance: • Alert sent **within >1 minute and <=3 minutes** of 'Lower Performance'/'Breach' conditions of 'Uptime Availability'	1% of Monthly Payment
		Breach: • **Alert sent >3 minutes** of 'Lower Performance'/'Breach' conditions of 'Uptime Availability'	2% of Monthly Payment
Support Channels – Incident and Helpdesk			
Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels.	Baseline: **95% of tickets/incident within 15 minutes** **(Rounded off to next higher value)**	No Penalty
		Low Performance:	5 % of the monthly payment)

	This is calculated for all tickets/incidents reported within the reporting month	**< 95 % &> = 85 %** **(Rounded off to next higher value)**	
		Breach: < 85 % **(Rounded off to next higher value)**	10 % of monthly payment
Time to Resolve - Severity 1 .	Time taken to resolve the reported ticket/incident from the time of logging.	Baseline: For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting **(Rounded off to next higher value)**	No Penalty
		Low Performance: <98% &>=90% of the incidents are resolved within 30 minutes of problem reporting **(Rounded off to next higher value)**	5 % of monthly payment
		Breach: < 90% of the incidents are resolved within 30 minutes of problem reporting **(Rounded off to next higher value)**	10 % of monthly payment
Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	Baseline: 95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting	No Penalty

		(Rounded off to next higher value)	
		Low Performance: < 95 % and > = 90 % of Severity 2 within 4 hours of problem reporting AND < 95 % and > = 90 % of Severity 3 within 16 hours of problem reporting **(Rounded off to next higher value)**	5 % of monthly payment
		Breach: < 90 %of Severity 2 within 4 hours of problem reporting AND < 90 % of Severity 3 within 16 hours of problem reporting **(Rounded off to next higher value)**	10 % of monthly payment

Please note:

1. Bidder shall provide an uptime as mentioned in the above table for the provisioned cloud services, which shall be **calculated on monthly basis. The Uptime is equal to total hours in a month less downtime (excluding permitted downtime for maintenance).** The Downtime is the time between the non-availability of services and time of restoration of services within the contracted hours. **Permitted downtime will not be considered as downtime of the service.**
2. For Service Levels purpose a month will be treated as 30 days. **In case of breach, then BMTC shall have right to terminate the contract and forfeit Performance bank guarantee.** The selected bidder is required to implement the requisite tools to automatically generate reports on up-time.
3. CSP needs to monitor uptime of the hosted applications and provide the alert regarding any breach. Alert will be

triggered to relevant stakeholders from BMTC and application SI. Stakeholders will be notified when certain application is down, or certain business rule of hosting is breached.

4. The up-time SLA will be implemented **only during the maintenance phase.**
5. In case of breach, BMTC may issue a show cause notice seeking explanation from the MSP.
6. Definitions of the levels of incidents as mentioned in the above table are as below:
   - ✓ Severity 1: The security or performance related issues impacting the performance and leading to unavailability of the services across all the departments.
   - ✓ Severity 2: The security or performance related issues impacting the performance and leading to unavailability of the services in one or more departments.
   - ✓ Severity 3: The security or performance related issues impacting the performance and leading to unavailability of the services to one or more users in the departments.

7. PROJECT TIMELINES AND DELIVERABLES

Sl. No.	Milestone	Timeline	Activities	Deliverable by MSP
1	Issuance of Letter of Intent (LoI)	T0	Issuance of Letter of Intent (LoI) to MSP by BMTC	
2	Technical Solution	T0+ 7 days, T1	Preparation of Technical Solution Report by MSP consisting: Inception, consisting, but not limited to: 1. Overview of the project and scope of work	Technical Solution Report

			2. Project plan along with completion timelines 3. Manpower requirements Solution Architecture, consisting, but not limited to: 1. Cloud services being proposed along with detailed configuration 2. Design and Solution Architecture (covering compute, storage, network connectivity, security, integration points, etc.) 3. Details of performance monitoring tools 4. System capacity planning	
3	Review of Technical Solution Report by BMTC	T1+ 7 days, T2	Review by BMTC/it's SI and subsequent modification in report by MSP, if required	
4	Provisioning of cloud services	T0 + 30 days, T3	Provisioning and setup of cloud services by MSP as per the approved solution architecture.	
5	Deployment of application and testing	T3 + 20 days, T4	Application deployment in the cloud infrastructure by BMTC/its SI. UAT to be carried out by BMTC//it's SI with assistance from MSP and subsequent changes/issue resolution by MSP, if required	Full Testing Completion Report 1. Report with the details of various issues identified and mitigated during the UAT. 2. A final test report which indicates successful completion of the UAT.
6	Go Live	T4	Successful completion of UAT will be	Go-Live report indicating

	(at successful completion of UAT)		treated as the criterion for Go-Live.	successful completion of solution implementation and Go-Live of the solution
7	Stabilization Phase (SLA Holiday period)	T4 + 60 days, T5	The MSP shall support BMTC/its SI in monitoring the Cloud Infrastructure for the stabilization period of 60 days after Go-Live.	
8	Maintenance of cloud services	T5 + 48 Months, T10	Activities such as: ✓ Support for all the components (upgrades, updates, call, escalation, response time, resolution time) ✓ Maintaining the helpdesk for Cloud components ✓ Support during the Operations phase for any error correction or version Updation ✓ Provisioning of new VM deletion, Updation, etc.	

8. **PAYMENT SCHEDULE AND MILESTONE**

All the payments will be done to the selected Service Provider by the BMTC after the delivery of services. Following payment milestones shall be applicable for the Cloud Services Consumed:

Sl. No.	Payment Phase	Milestone	Amount
1.	Monthly Payments (The first payment will be due on completion of one month (30 days) from the Go-Live date)	At the end of each Month after satisfactory delivery of the services and acceptance of the submitted invoice to BMTC.	Payment will be based on the **actual usage measured of the services** and as per the "Unit Costs" under Financial Bid. The overall cap for any monthly payment will be the monthly amount as per the Bill of Material (BoM) quoted by the MSP. If the billing period is less than one month, then amount will be calculated on pro-rata basis and for this purpose the following factors are considered □ One month is equal to 30 days □ One day consists of 24 hours □ One hour consists of 60 minutes

Disbursement of payment to the Bidder is based on completion of tasks indicated in the implementation plan; Operations and maintenance support plan and final handing over of O&M to the third party on completion at the end of the contractual period.

Notes:

- ✓ Payment shall be made on Monthly Basis.
- ✓ Payment shall be made in INR.
- ✓ Adherence to timelines is critical for the success of the project.
- ✓ Monthly Recurring Cost shall be paid post the Service rendered by MSP.
- ✓ If the Bidder is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same will be adjusted from the payments.
- ✓ BMTC will release the payment within 30days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the project and meeting the SLA Criteria. BMTC shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by Bidder, when BMTC disputes such invoice or part of it, provided that such dispute is Bonafede.

- ✓ No payment made by BMTC herein shall be deemed to constitute acceptance by BMTC of the system or any service.
- ✓ If the Bidder is liable for any penalty/liquidated damages as per the SLA, the same shall be adjusted from monthly payments due to the service provider.
- ✓ All payments shall be made corresponding to the services actually delivered, installed, or operationally accepted, as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.
- ✓ All Invoices should be supported with the full set of service level reports.

Payment for MSP:

I. For payment, the invoice with relevant documents such as Acceptance Certificate and Go-Live Report should be submitted to CSM, BMTC.

II. All payments shall be made after adjusting the penalty deductible, if any.

III. The BMTC shall make above payment directly in the Account of successful bidder. To make payment directly through Bank, the bidders are requested to furnish following information in respect of their Bank Account: -

- ✓ Name of Bank and address of branch.
- ✓ Their Bank Account Number.
- ✓ IFS code of the Branch for RTGS transfer.
- ✓ Charges required by Bank in this regard will be debited to suppliers'/contractors' Account. Net payment after deduction of charges required by the Bank shall be released in favour of success full bidders.

9. **HELP DESK AND SUPPORT**

- ✓ Service provider shall provide the Call logging & Help Desk support on 24*7 for all services.

SECTION 6: ANNEXURES

ANNEXURE 1: RESOURCE PROFILES FOR MSP TEAM
O&M Phase

S. No	Profile	Number	Min. Edu. Qualification	Experience	Responsibilities
1	Cloud Infrastructure Admin	2	Degree in Engineering /BCA/ MCA/BSc/ MSc Certification: Certified by any major CSP	Minimum of 5 years of Data Centre experience including 3 years of Cloud Infrastructure Administration	✓ Responsible for Cloud infrastructure uptime including Virtual Machines, Cloud solution ✓ Provisioning and de-provisioning of VMs ✓ Incident Resolution, Request resolution ✓ VM monitoring, administration, Back-up and restoration and reporting ✓ Plan &implement comprehensive security policies and practices on VM's, Virtualization Layer in cloud infrastructure. ✓ Knowledge of containerization ✓ Setting up CI/CD pipelines ✓ Experience in docker containers
2	Project Manager	1	Degree in Engineering /BCA/ MCA/BSc/ MSc Preferable:	✓ At least 10 years of work experience in managing	✓ Overall responsibility for executing the project including: ✓ Managing the

S. No	Profile	Number	Min. Edu. Qualification	Experience	Responsibilities
			PMP / Prince2 Certification	IT project delivery ✓ Experience in managing cloud service and deployment	implementation activities, tracking progress and SLAs ✓ Supervising the team of resources ✓ Reporting project progress and issues/escalations to BMTC Project Team

ANNEXURE 2: CHANGE CONTROL NOTE FORMAT

Change Control Note	CCN Number:
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications)	
Authorized by:	Date:
Name:	
Signature: Received by the IP	Date:
Name:	
Signature:	
Change Control Note	CCN Number:
Part B: Evaluation	
Changes to Services, charging structure, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.	
Brief Description of Solution:	
Impact:	
Deliverables:	
Timetable:	
Charges for Implementation: (Including a schedule of payments)	
Other Relevant Information: (Including value-added and acceptance criteria)	
Authorized by the Implementation Partner	Date:
Name:	
Signature:	

BANGALORE METROPOLITAN TRANSPORT CORPORATION

Tender No: BMTC/2023-24/SE0074 Date:14.06.2023

SELECTION OF MANAGED SERVICE PROVIDER (MSP) FOR CLOUD SERVICES TO BMTC

Request for Proposal
Volume II
JUNE -2023

Bangalore Metropolitan Transport Corporation
Kengal Hanumanthaiah Road, Shanthinagar
Bangalore 560027

CONTRACT FOR MANAGED SERVICE PROVIDER'S SERVICES

Bangalore Metropolitan Transport Corporation

Kengal Hanumanthaiah Road, Shanthinagar

Bangalore 560027

And

.....

Dated: ...../ ...../.....

I. FORM OF CONTRACT

This CONTRACT (hereinafter called the "Contract") is made the _____ day of the month of _____, 2023, between, on the one hand, BMTC Central Office, Kengal Hanumanthaiah Road, Shanthinagar, Bangalore 560027 (hereinafter called the "Client") represented by ---------- and on the other hand, _____(hereinafter called the " Managed Service Provider" – Name and Full address) represented by .....(Name and Designation)

WHEREAS

The Client has requested the Managed Service Provider to provide certain services as defined in the General Conditions of Contract attached to this Contract (hereinafter called the "Services");

The Managed Service Provider, having represented to the Client that they have the required professional skills, and personnel and technical resources, have agreed to provide the Services on the terms and conditions set forth in this Contract; and

NOW THEREFORE the parties hereto hereby agree as follows:
The following documents attached hereto shall be deemed to form an integral part of this Contract:

(a) The General Conditions of Contract (hereinafter called "GCC");
(b) The Special Conditions of contract (hereinafter called "SCC");
(c) The following Appendices:

Appendix A:	Description of the Services
Appendix B:	Reporting Requirements
Appendix C:	Key Personnel
Appendix	Duties of the Client

D:
Appendix Cost Estimates
E:

FOR AND ON BEHALF OF [NAME OF THE CLIENT]

By

(Authorized Representative)

FOR AND ON BEHALF OF [NAME OF THE MANAGED SERVICE PROVIDER]

By

(Authorized Representative)

II. GENERAL CONDITION OF CONTRACT (GCC)

1. GENERAL PROVISIONS

1.1. DEFINITION

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

a. "Applicable Law" means the laws and any other instruments having the force of law in India, as they may be issued and in force from time to time;
b. "Contract" means the Contract signed by the Parties, to which these General Conditions of Contract (GCC) are attached, together with all the documents listed in Clause 4 of such signed Contract;
c. “Effective Date” means the date on which this Contract comes into force;
d. “Contract Price” means the price to be paid for the services in accordance to clause 6
e. "GCC" means these General Conditions of Contract;
f. "Government" means the Government of Karnataka;
g. "Local currency" means Indian National Rupee;
h. "Party" means the Client or the Managed Service Provider, as the case may be, and Parties means both of them;
i. "Personnel" means persons hired by the Managed Service Provider as employees and assigned to the installation or Services or any part thereof; and ‘key personnel’ means the personnel referred to in Appendix A
j. "SCC" means the Special Conditions of Contract by which these General Conditions of Contract may be amended or supplemented;

k. "Services" means work to be performed by the Managed Service Providers pursuant to this Contract as described in Appendix A; and
l. 'Third party" means any person or entity other than the Government, the Client, the Managed Service Provider;

1.2. LAW GOVERNING THE CONTRACT

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Law.

1.3. LANGUAGE

This Contract has been executed in English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.4. NOTICES

Any notice, request or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to any authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, electronic mail, telex or facsimile to such Party at the address specified below:

The addresses are:
Client: BMTC Central Office, Kengal Hanumanthaiah Road, Shanthinagar, Bangalore 560027
Successful Managed Service Provider: _____

Notice shall be deemed to be effective as follows:

- in the case of personal delivery or registered mail, on delivery;
- in the case of telexes/e-mail, 24 hours following confirmed transmission;
- in the case of telegrams, 24 hours following confirmed transmission; and
- in the case of facsimiles, 24 hours following confirmed transmission

1.5. LOCATION

The locations of services to be provided by successful Managed Service Provider is set out in the RFP–Section 5: Terms of Reference/any amendments done post pre-proposal conference by client and, where the location of a task is not so specified, at such locations, whether in Karnataka or elsewhere, as the Client may approve.

1.6. AUTHORIZED REPRESENTATIVES

Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Client or the successful Managed Service Provider may be taken or executed by the following officials:

For the Client: Controller of Stores and Purchases

For the Successful Managed Service Provider:

_____

1.7. TAXES AND DUTIES

The Successful Managed Service Provider shall pay such taxes, duties, fees, licenses, statutory payments and contributions to employees as per applicable laws (including labour laws) and other impositions as may be levied under the Applicable Law, the amount of which is deemed to have been included in the Contract Price. The Contract shall be interpreted in accordance with the laws of the Union of India.

1.8. CONDITIONS PRECEDENT

1.8.1. PROVISIONS TO TAKE EFFECT UPON FULFILMENT OF CONDITIONS PRECEDENT

Subject to express terms to the contrary, the rights and obligations under this Agreement shall take effect only upon fulfilment of all the Conditions Precedent set out below. However, Client or its nominated agencies may at any time at its sole discretion waive fully or partially any of the Conditions Precedent for the Service Provider. For the avoidance of doubt, it is expressly clarified that the obligations of the Parties (or its nominated agencies) under this Agreement shall commence from the fulfilment of the Conditions Precedent as set forth below

1.8.2. CONDITIONS PRECEDENT OF THE MANAGED SERVICE PROVIDER

The Managed Service Provider shall be required to fulfil the Conditions Precedent which is as follows:

a) to provide a Performance Security/Guarantee and other guarantees/ payments with the date specified in the letter of acceptance from the Client; and
b) to provide the Client or its nominated agencies certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery and performance of this Agreement by the Managed Service Provider.

1.8.3. CONDITIONS PRECEDENT OF THE CLIENT

The Client shall be required to fulfil the Conditions Precedents which are as follows:

a) Necessary clearances associated with the execution of the project, unless specified to be performed by the Service Provider.
b) Approval of the Project by a Competent Authority, etc.

1.8.4. EXTENSION OF TIME FOR FULFILMENT OF CONDITIONS PRECEDENT

The Parties may, by mutual agreement extend the time for fulfilling the Conditions Precedent and the Term of this Agreement.

1.8.5. NON-FULFILMENT OF THE SERVICE PROVIDER'S CONDITIONS PRECEDENT

a) In the event that the Agreement fails to come into effect on account of non-fulfilment of the Service Provider's Conditions Precedent, the Client or its nominated agencies shall not be liable in any manner whatsoever to the Managed Service Provider and the Client shall forthwith forfeit the Earnest Money Deposit, if taken.
b) In the event that possession of any of the Client or its nominated agencies facilities has been delivered to the Managed Service Provider prior to the fulfilment of the Conditions Precedent, upon the termination of this Agreement such shall immediately revert to Client or its nominated agencies, free and clear from any encumbrances or claims.

1.9. CHANGE OF CONTROL

a) In the event of a change of control of the Managed Service Provider during the Term, the Managed Service Provider shall promptly notify Client and/or its nominated agencies of the same.
b) If the net worth of the surviving entity is less than that of Managed Service Provider prior to the change of control, the Client or its nominated agencies may within 30 days of becoming aware of such change in control, require a replacement of existing Performance Guarantee furnished by the Managed Service Provider from a guarantor acceptable to the Client or its nominated agencies (which shall not be Managed Service Provider or any of its associated entities).
c) If such a guarantee is not furnished within 30 days of the Client or its nominated agencies requiring the replacement, the Client may exercise its right to terminate this Agreement within a further 30 days by written notice, to become effective as specified in such notice.
d) Pursuant to termination, the effects of termination as set out in Clause 2.7 of this Agreement shall follow.
e) For the avoidance of doubt, it is expressly clarified that the internal reorganization of the Managed Service Provider shall not be deemed an event of a change of control for purposes of this Clause unless the surviving entity is of less net worth than the predecessor entity.

1.10. REPRESENTATIONS AND WARRANTIES

1.10.1. REPRESENTATIONS AND WARRANTIES OF THE SERVICE PROVIDER

The Managed Service Provider represents and warrants to the Client or its nominated agencies that:

a) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and other agreements and to carry out the transactions contemplated hereby;
b) it is a competent provider of a variety of Cloud and managed services;
c) it has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and delivery

of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

d) from the Effective Date, it will have the financial standing and capacity to undertake the Project in accordance with the terms of this Agreement;
e) in providing the Services, it shall use reasonable endeavours not to cause any unnecessary disruption to Client's normal business operations;
f) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms hereof;
g) the information furnished in the Managed Service Provider’s response to the RFP and any subsequent clarification pertaining to the evaluation process, furnished on or before the date of this Agreement is to the best of its knowledge and belief true and accurate in all material respects as at the date of this Agreement;
h) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;
i) there are no material actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its material obligations under this Agreement;
j) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;
k) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement;
l) no representation or warranty by it contained herein or in any other document furnished by it to Client or its nominated agencies in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading; and

m) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of Client or its nominated agencies in connection therewith.

1.10.2. REPRESENTATIONS AND WARRANTIES OF THE CLIENT OR ITS NOMINATED AGENCIES

Client or its nominated agencies represent and warrant to the Managed Service Provider that:

a) it has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby;
b) it has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;
c) it has the financial standing and capacity to perform its obligations under the Agreement;
d) it is subject to the laws of India, and hereby expressly and irrevocably waives any immunity in any jurisdiction in respect of this Agreement or matters arising there under including any obligation, liability or responsibility hereunder;
e) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms thereof;
f) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;
g) there are no actions, suits or proceedings pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the default or breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform its material (including any payment) obligations under this Agreement;
h) it has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on the Client or its nominated agencies ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such

proceedings that would adversely affect the performance of its obligations under this Agreement;

i) it has complied with Applicable Laws in all material respects;
j) all information provided by it in connection with the Project is, to the best of its knowledge and belief, true and accurate in all material respects; and
k) upon the Managed Service Provider performing the covenants herein, it shall not at any time during the term hereof, interfere with peaceful exercise of the rights and discharge of the obligations by the Service Provider, in accordance with this Agreement.

2. COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

2.1. EFFECTIVENESS OF CONTRACT

This Contract shall come into effect on the date the Contract is signed by both the Parties.

2.2. COMMENCEMENT OF SERVICES

The Managed Service Provider shall begin carrying out the "Services" after the issuance of LOI/Work Order.

2.3. EXPIRATION OF CONTRACT

Unless terminated earlier pursuant to Clause 2.7, this Contract shall terminate at the end of such time **period after the completion of a period of 48 months from the Go-Live date.**

2.4. MODIFICATION

Modification of the terms and conditions of this Contract, including any modification of the Rent or of the Contract Price, may only be made by written agreement between the Parties.

2.5. FORCE MAJEURE

2.5.1. DEFINITION OF FORCE MAJEURE

"Force Majeure" shall mean any event beyond the reasonable control of either Party, as the case may be, and which is unavoidable notwithstanding the reasonable care of the Party affected.

2.5.2. Force Majeure events

i. A Force Majeure shall include, without limitation, the following:
   a. war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war; strike, lockout (strike and lockout not caused due to either Party's default), sabotage embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;
   b. earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

epidemic, pandemic, major public health disaster;

ii. If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within five (5) days after the occurrence of such event.

iii. The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The time for achieving Final Acceptance shall be extended.

iv. The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfil its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract.

v. No delay or non-performance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:
   a. constitutes a default or breach of the Contract;
   b. give rise to any claim for damages or additional cost or expense occasioned by the delay or non-performance, if, and to the extent that, such delay or non-performance is caused by the occurrence of an event of Force Majeure.

vi. If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

vii. In the event of termination pursuant to material breach, the rights and obligations of the Managed Service Provider and Purchaser shall be as specified in the clause titled Termination.

viii. For the avoidance of doubt, it is expressly clarified that the failure on the part of the selected Managed Service Provider under this Agreement or the service levels to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of this Agreement or the service levels against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event. For the avoidance of doubt, it is further clarified that any negligence in performance of Services which directly causes any breach of security like hacking aren't the forces of nature and hence wouldn't be qualified under the definition of "Force Majeure". In so far as applicable to the performance of Services, Managed Service Provider will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes and technology to prevent any breach of security and any resulting liability there from (wherever applicable).

ix. For the Managed Service Provider to take benefit of this clause,

it is a condition precedent that the Managed Service Provider must promptly notify Purchaser, in writing of such conditions and the cause thereof within five calendar days of the arising of the Force Majeure event. Purchaser, or the consultant / committee appointed by Purchaser shall study the submission of the Managed Service Provider and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by Purchaser in writing, the Managed Service Provider shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

x. In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, Purchaser and the Managed Service Provider shall hold consultations with each other in an endeavour to find a solution to the problem.

xi. Notwithstanding anything to the contrary mentioned above, the decision of Purchaser shall be final and binding on the Managed Service Provider.

2.6. SUSPENSION

The Client may by written notice of suspension to the Service Provider, suspend all payments to the Managed Service Provider hereunder, if the Managed Service Provider fail to perform any of their obligations under this contract, including the carrying out of the Services, provided that such notice of suspension

a. shall specify the nature of the failure, and
b. shall request the Managed Service Provider to remedy such failure within a period not exceeding thirty (30) days after receipt by the Managed Service Provider of such notice of suspension.

2.7. TERMINATION

2.7.1. CLIENT

The Client may terminate this Contract, by not **less than thirty (30) days' written** notice of termination to the Managed Service Provider, to be given after the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause 2.7.1 and **sixty (60) days in the case of the event referred to in (f):**

a) if the Managed Service Provider do not remedy a failure in the performance of their obligations under the Contract, within thirty (30) days of receipt after being notified or within such further period as the Client may have subsequently approved in writing;
b) if the Managed Service Provider (or any of their members) become insolvent or bankrupt;
c) if, as the result of Force Majeure, the Managed Service Provider are unable to perform a material portion of the Services for a period of not less than sixty (60) days; or
d) if it comes to the Client's attention that the Managed Service Provider (or the MSP's Team) is in a position of actual conflict of

interest with the interests of the Client, in relation to any of terms of MSP's Bid, the RFP or this Contract.

e) Where a change of management of the Managed Services Provider has occurred whereby MSP's company is merged, amalgamated or has been taken over, due to which the majority shareholding of MSP has been transferred to another entity and the Client has ascertained based on facts that the new entity is materially deficient in technical and financial capacity compared to the original company and this is likely to materially adversely affect the Project, the Client may terminate this contract by serving the termination notice to MSP and therewith give a reasonable opportunity to MSP to explain its position on the matter and thereupon give **two (2) month's cure period to MSP for rectifying the situation. In case the MSP** fails to rectify the situation, the Client will have the option to terminate the contract without any compensation damages whatsoever and invoke the Performance Bank Guarantee.

f) if the Service Provider, in the judgment of the Client has engaged in corrupt or fraudulent practices in competing for or in executing the Contract. For the purpose of this clause: "corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the selection process or in contract execution. "Fraudulent practice" means a misrepresentation of facts in order to influence a selection process or the execution of a contract to the detriment of the Client/GOK, and includes collusive practice among Managed Service Provider (prior to or after submission of proposals) designed to establish prices at artificial non-competitive levels and to deprive the Client/GOK of the benefits of free and open competition.

2.7.2. BY THE MANAGED SERVICE PROVIDER

a) The Managed Service Provider may terminate this Contract, by not less than thirty (30) days' written notice to the Client, such notice to be given after the occurrence of any of the events specified in paragraphs (i) through (iii) of this Clause 2.7.2:

(I) if the Client fails to pay any money due to the Managed Service Provider pursuant to this Contract and not subject to dispute pursuant to Clause 7 hereof within forty-five (45) days after receiving written notice from the Managed Service Provider that such payment is overdue;

(II) If the Client is in material breach of its obligations pursuant to this Contract and has not remedied the same with in forty-five (45) days (or such longer period as the Managed Service Provider may have subsequently approved in writing) following the receipt by the Client of the Managed Service Provider' notice specifying such breach;

(III) if, as the result of Force Majeure, the Managed Service Provider are unable to perform a material portion of the Services for a period of not less than sixty (60) days.

2.7.3. CESSATION OF RIGHTS AND OBLIGATIONS

Upon termination of this Contract pursuant to Clause GCC 2.7, or upon expiration of this Contract pursuant to Clause GCC 2.3, all rights and obligations of the Parties hereunder shall cease, except:

a) Such rights and obligations as may have accrued on the date of termination or expiration;
b) The obligation of confidentiality set forth in Clause GCC 3.3 hereof;
c) Any right which a Party may have under the Applicable Law.

2.7.4. CESSATION OF SERVICES

Upon termination of this Contract by notice of either Party to the other pursuant to Clauses GCC 2.7.1 or GC 2.7.2 hereof, the Managed Service Provider shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum. With respect to documents prepared by the Managed Service Provider and equipment and materials furnished by the Client, the Managed Service Provider shall proceed as provided, respectively, by Clauses GCC 3.7, GCC 3.8 and GCC 3.10

2.7.5. PAYMENT UPON TERMINATION

Upon termination of this Contract pursuant to Clauses 2.7.1 or 2.7.2, the Client shall make the following payments to the Managed Service Provider: (a) remuneration pursuant to Clause 6 for Services satisfactorily performed prior to the effective date of termination; (b) except in the case of termination pursuant to paragraphs (a) and (b) of Clause 2.7.1, reimbursement of any reasonable cost incident to the prompt and orderly termination of the Contract.

3. OBLIGATIONS OF SERVICE PROVIDER

3.1. GENERAL

The Managed Service Provider shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The Managed Service Provider shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the Client, and shall at all times support and safeguard the Client's legitimate interests in any dealings with Sub Managed Service Provider or third parties.

3.2. CONFLICT OF INTEREST

3.2.1. MANAGED SERVICE PROVIDER NOT TO BENEFIT FROM COMMISSIONS, DISCOUNTS, ETC.,

The remuneration of the Managed Service Provider pursuant to Clause 6.1 shall constitute the Service Provider' sole remuneration in connection with this Contract or the Services, and the Managed Service Provider shall not accept for their own benefit any trade commission, discount or similar payment in connection with activities pursuant to this Contract or to the Services or in the

discharge of their obligations under the Contract, and the Managed Service Provider shall use their best efforts to ensure that the Personnel, any Sub-Service Provider, and agents of either of them, similarly shall not receive any such additional remuneration.

3.2.2. PROCUREMENT RULES OF FUNDING AGENCIES

If the Service Provider, as part of the Services, have the responsibility of advising the Client on the need assessment on procurement of goods, works or services, the Managed Service Provider shall comply with any applicable procurement guidelines of the funding agencies and shall at all times exercise such responsibility in the best interest of the Client.

3.2.3. MANAGED SERVICE PROVIDER AND AFFILIATES NOT TO ENGAGE IN CERTAIN ACTIVITIES

The Managed Service Provider agree that, during the term of this Contract and after its termination, the Managed Service Provider and their affiliates, shall be disqualified from providing goods, works or services (other than the Services and any continuation thereof) for any project resulting from or closely related to the Services.

3.2.4. PROHIBITION OF CONFLICTING ACTIVITIES

Neither the Managed Service Provider nor their Sub-Managed Service Provider nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

a) During the term of this Contract, any business or professional activities in the Government's country which would conflict with the activities assigned to them under this Contract; or
b) After the termination of this Contract, such other activities as may be specified in the SCC.

3.3. CONFIDENTIALITY

The Service Provider, their Sub-Service Provider, and the Personnel of either of them shall not, either during the term or within two (2) years after the expiration of this Contract, disclose any proprietary or confidential information or Evaluation report relating to the Project, the Services, this Contract, or the Client's business or operations without the prior written consent of the Client.

3.4. INSURANCE TO BE TAKEN OUT BY THE MANAGED SERVICE PROVIDER

o This clause deleted.

3.5. SERVICE PROVIDER’S ACTIONS REQUIRING CLIENT’S PRIOR APPROVAL

The Managed Service Provider shall obtain the Client’s prior approval in writing before taking any of the following actions:

a) entering into a subcontract for the performance of any part of the Services
b) appointing such members of the Personnel not listed by name in Appendix C (“Key Personnel”), and
c) any other action that may be specified in the SCC.

3.6. REPORTING OBLIGATIONS

The Managed Service Provider shall submit to the Client the reports and documents specified and within the periods set forth in the said RFP.

3.7. DOCUMENTS PREPARED BY THE MANAGED SERVICE PROVIDER TO BE THE PROPERTY OF THE CLIENT

- All plans, drawings, specifications, designs, reports and other documents and Evaluation report submitted by the Managed Service Provider in accordance with **Clause 3.6** shall become and remain the property of the Client, and the Managed Service Provider shall, not later than upon termination or expiration of this Contract, deliver all such documents and evaluation report to the Client, together with a detailed inventory thereof. The Managed Service Provider shouldn't retain a copy of such documents and report or give an undertaking on Restrictions about the future use of such documents.
- The client shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have solely arisen out of or have been developed solely during execution of the Agreement, including but not limited to all processes, products, specifications, reports, drawings and other documents which have been newly created and developed by the Managed Service Provider solely during the performance of the Services / delivery of Products and for the purposes of, inter-alia, use or sub-license of such Services under the Contract. The Managed Service Provider undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the client and execute all such agreements/documents and file all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the client
- Any / all Intellectual Property owned by the client prior to the execution date and/ or any Intellectual Property Right applied for prior to the execution date shall strictly vest with the client and the Managed Service Provider shall have no right whatsoever on such Intellectual Property.
- Pre-existing work: All intellectual property rights existing prior to the date of execution of the agreement shall belong to the Party that owned such rights immediately prior to such date.
- Third Party Products: If assignment / license agreements are necessary or appropriate between the Managed Service Provider and third parties for purposes of enabling / enforcing / implementing the provisions hereinabove, the Managed Service Provider shall enter into such agreements at its own sole cost, expense and risk and all such assignments / licenses etc.
- The Managed Service Provider shall not use the Client licensing credentials for the purpose of providing support services to any other client. In case the Managed Service Provider is found to be involved in such act, Client reserves the right to impose the penalty and may terminate the Contract.

3.8. EQUIPMENT AND MATERIALS FURNISHED BY THE CLIENT

This clause is deleted.

3.9. USE OF ASSETS BY THE MANAGED SERVICE PROVIDER

During the Term, the Managed Service Provider shall:

a) take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the Project and other facilities leased / owned / operated by the Managed Service Provider exclusively in terms of ensuring their usability for the delivery of the Services as per this Agreement (hereinafter the "Assets") in proportion to their use and control of such Assets; and

b) keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) as at the date the Managed Service Provider takes control of and/or first uses the Assets and during the entire Term of the Agreement.

c) ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and which are provided to the Managed Service Provider will be followed by the Managed Service Provider and any person who will be responsible for the use of the Assets;

d) take such steps as may be properly recommended by the manufacturer of the Assets and notified to the Managed Service Provider or as may, in the reasonable opinion of the Service Provider, be necessary to use the Assets in a safe manner;

e) ensure that the Assets that are under the control of the Service Provider, are kept suitably housed and in conformity with Applicable Law;

f) not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to Applicable Law.

3.10. TRANSFER OF ASSETS

3.10.1. TRANSFER OF ASSET REGISTER

I. Six (6) months prior to expiry or within 2 (two) weeks of notice of termination of the Agreement the Managed Service Provider shall deliver to the Client :
   a) Complete client data.
   b) Complete client applications deployed.
   c) Migration plan.
   d) Any configuration details related to client applications and database.

3.10.2. TRANSFER OF DOCUMENTATION

Six (6) months prior to expiry or within two (2) weeks of notice of termination of the Agreement the Managed Service Provider shall deliver to the Client a full, accurate and up-to date set of Documentation that relates to any element of the Project.

3.10.3. TRANSFER OF SERVICE MANAGEMENT PROCESS

Six (6) months prior to expiry or within two (2) weeks of notice of termination of the Agreement, the Managed Service Provider shall

deliver to the Client:

(a) a plan for the handover and continuous delivery of the Service Desk function and allocate the required resources;

(b) full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:

i. Incidents;
ii. Problems;
iii. Service Requests;
iv. Service Level reporting data;

3.10.4. TRANSFER OF KNOWLEDGE BASE

Six (6) months prior to expiry or within two (2) weeks of notice of termination of the Agreement the Managed Service Provider shall provide required knowledge transfer for migration support.

3.10.5. TRANSFER OF DATA

i. In the event of expiry or termination of the Agreement, the Managed Service Provider shall cease to use the Client data and, at the request of the Client, shall destroy all such copies of the Client data then in its possession to the extent specified by the Client.

ii. Except where, pursuant to clause 3.10.5 (i) above, the Client has instructed the Managed Service Provider to destroy such Client Data as is held and controlled by the Service Provider, one (1) month prior to expiry or within one (1) month of termination of the Agreement, the Managed Service Provider shall deliver to the Client:

a) an inventory of the Client data held and controlled by the Service Provider, plus any other data required to support the Services; and/or

b) A draft plan for the transfer of the Client data held and controlled by the Managed Service Provider and any other available data to be transferred.

3.10.6. TRANSFER OF SUPPORT ACTIVITIES

Six (6) months prior to expiry or within ten (10) Working Days of issue of notice of termination, the Managed Service Provider shall assist the Client or Replacement Managed Service Provider to develop a viable exit transition plan which shall contain details of the tasks and responsibilities required to enable the transition from the Services provided under the Agreement to the Replacement Managed Service Provider or the Client, as the case may be.

i. The exit transition plan shall be in a format to be agreed with the Client and shall include, but not be limited to:
   a) a timetable of events;
   b) resources;
   c) assumptions;
   d) activities;
   e) responsibilities; and
   f) risks.

ii. The Managed Service Provider shall supply to the Client or a Replacement Managed Service Provider specific material including but not limited to:

a) Change Request log;
b) entire back-up history; and
c) dump of database contents including the Asset Register, problem management system and operating procedures. For the avoidance of doubt this shall not include proprietary software tools of the Managed Service Provider which are used for project management purposes generally within the Service Provider's business.

iii. The Managed Service Provider shall provide, the Client or Replacement Managed Service Provider, proposal for the retention of Key Personnel for the duration of the transition period.

3.11. INFORMATION SECURITY

One of the most critical issues that need to be addressed in the Cloud Contract / Agreement is the security of the data and application. The level of sensitivity of data requires different controls to be put in place in the Cloud to prevent a compromise.

3.11.1. COMPLIANCES AND CERTIFICATIONS

i. As part of the empanelment process, the client has mandated CSPs to have certifications mentioned in the eligibility criteria of the RFP document. The Managed Service Provider shall ensure the sustenance of the above certificates and compliances applicable to the underlying CSPs during the entire duration of the project.

ii. If the Client has financial and payment related data that is proposed to be hosted on the Cloud, the Managed Service Provider shall provide Payment Card Industry Data Security Standard (PCI DSS) compliant technology infrastructure of underlying CSP for storing, processing, and transmitting payment related information in the Cloud. This standard is required if the transactions involve credit card payments.

iii. CSPs are

a) The Managed Service Provider shall ensure that the underlying CSP complies or meets any security requirements applicable to it either published (or to be published) by the Client or any standards body setup / recognized by Government of India from time to time and notified to the Managed Service Provider/ MeitY empanelled CSP as a mandatory guideline / standard.

b) The Managed Service Provider shall meet all the security requirements indicated in the IT Act 2000 and rules & regulations as amended from time to time. The underlying CSP shall meet all terms and conditions of the Empanelment of Cloud Service Offerings of Cloud Managed Service Provider and shall continuously comply with the audit criteria defined.

3.11.2. PRIVACY AND SECURITY SAFEGUARDS

i. The Managed Service Provider hall implement reasonable and appropriate measures to secure the Client’s data and content against accidental or unlawful loss, access or disclosure.

ii. Data to be retained throughout contract period.
iii. The Managed Service Provider cannot share or use data for purposes other than services mentioned in this RFP.
iv. Data can be shared only by BMTC, based on BMTC data sharing policy.
v. The Managed Service Provider shall report to the Client, in writing, of information security breaches by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.
vi. The Managed Service Provider shall undertake to treat information passed on to it under this Agreement/Contract as classified. Such Information shall not be communicated / published / advertised by the Managed Service Provider to any person/organization without the express permission of the Client.
vii. The Managed Service Provider shall not use/process the service attributes and data associated with Cloud and services for the purposes beyond the scope of the current project.

3.11.3. CONFIDENTIALITY

i. The Managed Service Provider shall maintain confidentiality, integrity, availability and privacy of the Client data. The Managed Service Provider shall execute Non-Disclosure Agreement (NDA) with the Client with respect to this Project. Following information is excluded from the NDA.
    a) information already available in the public domain;
    b) information which has been developed independently by the Service Provider;
    c) information which has been received from a third party who had the right to disclose the aforesaid information;
    d) Information which has been disclosed to the public pursuant to a court order.
ii. Disclosure of any part of the non-public information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law within India or other Statutory Authorities of Indian Government, could result in premature termination of the Agreement. The Client may apart from blacklisting the Service Provider, initiate legal action against the Managed Service Provider as per the applicable laws of India. The Managed Service Provider shall also not make any news release, public announcements, use of trademark or logo or any other reference on the Project, including application document / RFP, without obtaining prior written consent from the Client.
iii. The Managed Service Provider shall notify the Client as soon as possible in the event of an actual or suspected breach of data.
iv. The Managed Service Provider shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.
v. The Client or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action

against the Managed Service Provider regarding any forbidden disclosure.

vi. The Managed Service Provider shall ensure that all its employees, agents and sub-contractors involved in the Project, execute individual non-disclosure agreements, which have been duly approved by the Client with respect to this Project. The Managed Service Provider may submit a declaration that it has obtained the NDA from its employees. However, if the project is critical in nature, Managed Service Provider may get NDAs signed from every resource involved in the project and submit it to Client (Optional).

vii. Any handover of the confidential information needs to be maintained in a list, both by Client & Service Provider, containing at the very minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, mode of information, purpose and signatures of both parties.

viii. Notwithstanding anything to the contrary mentioned hereinabove, the Managed Service Provider shall have the right to share the Letter of Intent / work order provided to it by the Client in relation to this Agreement, with its prospective Clients solely for the purpose of and with the intent to evidence and support its work experience under this Agreement.

3.12. SERVICE LEVEL AGREEMENT

The Service Level Agreements (SLAs) mentioned in the RFP document under Section5. Data Sheet shall be applicable to Managed Service Provider and is part of this Agreement.

4. MANAGED SERVICE PROVIDER PERSONNEL

4.1. DESCRIPTION OF PERSONNEL

a) The titles agreed job descriptions, Type of resources and estimated periods of engagement in the carrying out of the Services of the Service Provider' Key Personnel are described in RFP and any other information shared by the client at the later stage.

b) The type of manpower to be deployed by the Successful Managed Service Provider for this project along with manpower replacement terms are stated in RFP Annexure 1.

c) It is the responsibility of the Successful Managed Service Provider to provide additional technical and administrative manpower, over and above the minimum manpower stated above, to meet the service level agreement requirements.

5. REMOVAL AND/OR REPLACEMENT OF PERSONNEL

a. Except as the Client may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Service Provider, it becomes necessary to replace any of the Key Personnel, the Managed Service Provider shall forthwith provide as a replacement a person of equivalent or better qualifications.

b. If the Client finds that any of the Personnel have (i) committed serious misconduct or has been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied

with the performance of any of the Personnel, then the Managed Service Provider shall, at the Client's written request specifying the grounds thereof, forthwith provide as a replacement a person with qualifications and experience acceptable to the Client.

c. The Managed Service Provider shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.
d. During the period of the contract, if the manpower deployed by the Successful Managed Service Provider is identified by the Client as incompetent, the Successful Managed Service Provider shall immediately remove such manpower from the project and provide alternate competent manpower of equivalent or better qualifications, within one week of receipt of such intimation.

6. OBLIGATION OF CLIENT

6.1. ASSISTANCE AND EXEMPTIONS

Unless otherwise specified in the SCC, the Client shall use its best efforts to ensure that the Government shall:

a) Issue circulars to officials, agents and representatives of the Government all such instructions as may be necessary or appropriate for the prompt and effective evaluation of the Services;

6.2. SERVICES AND FACILITIES

The Client shall make available to the Managed Service Provider and the Personnel, for the purposes of performing the services provided that if such facilities and required data shall not be made available to the Managed Service Provider as and when so specified, the Parties shall agree on; time extension that it may be appropriate to grant to the Managed Service Provider for the performance of the Services.

7. PAYMENT TO SERVICE PROVIDER

7.1. PAYMENT

As specified in the RFP section-5 of terms of reference.

7.2. CONTRACT PRICE

The Contract price is _____

7.3. PAYMENT FOR ADDITIONAL SERVICES

For the purpose of determining the remuneration due for additional services as may be agreed under **Clause 2.4, a breakdown of the lump sum price is provided in Appendix E.**

7.4. TERMS AND CONDITIONS OF PAYMENT

- Payments will be made to the account of the Managed Service Provider and according to the payment schedule stated below.
- The account is:
- Payment shall be made on ……
- All the payments will be done to the selected Service Provider by the BMTC after the delivery of services.
- Refer Section-5 of RFP for payment terms.

Deductions:

- The client shall be at liberty to deduct penalties/liquidated damages from the invoices raised by the Managed Service Provider as calculated by the client for non-adherence to Service Level Agreements.
- All payments to the Managed Service Provider shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which Client may have paid or incurred, for which under the provisions of the Contract, the Managed Service Provider is liable, the same shall be deducted by Client from any dues to the Service Provider. All payments to the Managed Service Provider shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by the Client to the Managed Service Provider on chargeable basis.
- Client shall provide the Managed Service Provider with the original tax receipt of any withholding taxes paid by Client or its nominated agencies on payments under the RFP after its payment. Managed Service Provider agrees to reimburse and hold Client or its nominated agencies harmless from and against any claims, losses, expenses (including attorney fees, court fees) etc. arising out of deficiency (including penalties and interest) in payment of taxes that is the responsibility of the Service Provider.

7.5. LIQUIDATED DAMAGES

- If the Managed Service Provider fails to deliver or fail to perform the Services within the period(s) specified in the Contract, the Client shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, 2% per week to a maximum up to 10% of contract value including tax.
- Once the maximum is reached, the client may consider termination of the Contract pursuant to Clause 2.7.1

8. SETTLEMENT OF DISPUTE

Normally there should not be any scope for dispute between the Client and the Managed Service Provider after into a mutually agreed valid contract. However due to various unforeseen reasons, problems may arise during the progress of the contract leading to disagreement between the Client and the Managed Service Provider.

8.1. Scope of Disputes

During the subsistence of this contract, the nature of dispute requiring resolution shall include but not limited to:

Managing Director, BMTC hereto arising out of or in connection with the validity, interpretation, implementation, material breach or any alleged material breach of any provision of this Contract or regarding any question, including as to whether the termination of this Contract by one Party hereto has been legitimate.

8.2. AMICABLE SETTLEMENT

The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.

Any dispute of either party, which cannot be settled amicably amongst themselves within thirty days of either party intimating it to the other party through writing, shall submit their dispute to the Managing Director, Bangalore Metropolitan Transport Corporation, who shall hear the dispute of the parties and pass the judgment, the orders of the Managing Director, BMTC shall be final.

8.3. DISPUTE SETTLEMENT

1. A Party claiming that a dispute has arisen must give the other Party to the dispute, notice setting out details of the dispute.
2. After a notice is given, each Party to the dispute must use its reasonable efforts to resolve the dispute.
3. If the Parties cannot resolve the dispute within reasonable period then any such dispute or difference whatsoever arising between the parties shall resolve the dispute before the Hon'ble Civil Court/Commercial Court at Bangalore.

8.4. GOVERNING LAW AND JURISDICTION

All disputes arising out of or in connection with this Contract shall be governed by the Indian laws for the time being in force, and as amended from time to time and the Civil Courts at Bangalore, India shall have jurisdiction over all matters arising out of or relating to this Agreement.

9. PERFORMANCE SECURITY

a) As detaile in earlier para.

10. INDEMNIFICATION & LIMITATION OF LIABILITY

a) Subject to Clause 9 (d) below, Managed Service Provider(the "Indemnifying Party") undertakes to indemnify, hold harmless the Client (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively "Loss") on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or wilful default in performance or non-performance under this Agreement.

b) If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

c) Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by
   i. Indemnified Party's misuse or modification of the Service;
   ii. Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party;
   iii. Indemnified Party's use of the Service in combination with any product or information not owned or developed by Indemnifying Party;
   iv. However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either
      a) Procure the right for Indemnified Party to continue using it
      b) Replace it with a non-infringing equivalent
      c) Modify it to make it no infringing.

The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.

d) The indemnities set out in Clause 9 shall be subject to the following conditions:
   i. the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;
   ii. the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Défense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Défense;
   iii. if the Indemnifying Party does not assume full control over the Défense of a claim as provided in this Article, the Indemnifying Party may participate in such Défense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses;
   iv. the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;
   v. all settlements of claims subject to indemnification under this Clause will:
      be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;
   vi. the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be

paid to it in connection with any such claim or proceedings;

- the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;
- in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates; and
- if a Party makes a claim under the indemnity set out under Clause 9 (a) above in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

e) The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the indemnification obligations set out in Clause 9

f) In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third-party claims (other than those set-forth in Clause 9 (a) even if it has been advised of their possible existence.

g) The allocations of liability represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

11. RISK PURCHASE

If the Managed Service Provider fails to perform its obligations (or any part thereof) under the Agreement or if the Agreement is terminated due to breach of any obligations and/or terms and conditions by the Managed Service Provider under the Agreement, the client reserves the right to procure the same or equivalent Services from alternative sources at the Service Provider’s risk and responsibility. Any incremental cost borne by the Client in procuring such Services shall be borne by the Service Provider. Any such incremental cost incurred in the procurement of such Services from alternative source will be recovered from the undisputed pending due and payable Payments /Security Deposit / Performance Bank Guarantee provided by the Managed Service Provider under the Agreement and if the value of the Services under risk purchase exceeds the amount of Security Deposit and / or Performance Bank

Guarantee, the same may be recovered, if necessary, by due legal process.

12. FORMAT FOR NON-DISCLOSURE AGREEMENT (NDA) (On INR 100/- Non-Judicial Stamp Paper)

This Non-Disclosure Agreement ("Non-Disc") is made and entered into_____day Of_____month_____year (effective date) by and between_____ ("Department") and_____ ("Company").

Whereas, Department and Company have entered into an Agreement ("Agreement") _____ Effective _____ for_____; and Whereas, each party desires to disclose to the other party certain information in oral or written form which is proprietary and confidential to the disclosing party, ("CONFIDENTIALINFORMATION").

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein, the parties agree as follows:

1. **Definitions.** As used herein:
   a) The term **"Confidential Information"** shall include, without limitation, all information and materials, furnished by either Party to the other in connection with citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer and prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document knowhow, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the disclosing party's data, computer database, products and/or services. Results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by the receiving party in connection with the Department's information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force shall also be considered Confidential Information.
   b) The term, **"Department"** shall include the officers, employees, agents, consultants, contractors and representatives of Department.
   c) The term, **"Company"** shall include the directors, officers,

employees, agents, consultants, contractors and representatives of Company, including its applicable affiliates and subsidiary companies.

2. **Protection of Confidential Information:** With respect to any Confidential Information disclosed to it or to which it has access, Company affirms that it shall:
   a. Use the Confidential Information as necessary only in connection with Project and in accordance with the terms and conditions contained herein;
   b. Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Information that the parties take to protect the confidentiality of its own proprietary and confidential information and that of its clients;
   c. Not to make or retain copy of any commercial or marketing plans, citizen/users/persons/customers database, Bids developed by or originating from Department or any of the prospective clients of Department except as necessary, under prior written intimation from Department, in connection with the Project, and ensure that any such copy is immediately returned to Department even without express demand from Department to do so;
   d. Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the other party; and
   e. Return to the other party, or destroy, at Department's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of (i) expiration or termination of either party's engagement in the Project, or (ii) the request of the other party therefore.
   f. Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between Department and Company and the nature of services to be provided by the Company to the Department.

3. **Onus.** Company shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoing exceptions.

4. **Exceptions.** These restrictions as enumerated in section 1 of this Agreement shall not apply to any Confidential Information:
   a. Which is independently developed by Company or lawfully received from another source free of restriction and without breach of this Agreement; or
   b. After it has become generally available to the public without breach of this Agreement by Agency; or
   c. Which at the time of disclosure to Company was known to such party free of restriction and evidenced by documentation

in such party's possession; or

d. Which Department agrees in writing is free of such restrictions.
e. Which is received from a third party not subject to the obligation of confidentiality with respect to such Information;

5. **Remedies.** Company acknowledges that (a) any actual or threatened disclosure or use of the Confidential Information by Company would be a breach of this agreement and may cause immediate and irreparable harm to Department; (b) Company affirms that damages from such disclosure or use by it may be impossible to measure accurately; and (c) injury sustained by Department may be impossible to calculate and remedy fully. Therefore, Company acknowledges that in the event of such a breach, Department shall be entitled to specific performance by Company of Company's obligations contained in this Agreement. In addition, Company shall indemnify Department of the actual and liquidated damages which may be demanded by Department. Moreover, Department shall be entitled to recover all costs (including reasonable attorneys' fees) which it or they may incur in connection with defending its interests and enforcement of legal rights arising due to a breach of this agreement by Company.

6. **Need to Know.** Company shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the disclosing party.

7. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

8. No Conflict. The parties represent and warrant that the performance of its obligations hereunder does not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

9. **Authority**. The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

10. **Dispute Resolution.**

If any difference or dispute arises between the Department and the Company in connection with the validity, interpretation, implementation or alleged breach of any provision of this

Agreement, any such dispute shall be referred to MD, BMTC.

11. **Governing Law.** All disputes arising out of or in connection with this Contract shall be governed by the Indian laws for the time being in force, and as amended from time to time and the Civil Courts at Bangalore, India shall have jurisdiction over all matters arising out of or relating to this Agreement.

12. Entire Agreement. This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

15. **Severability**. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

16. Waiver. If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after any expiration or termination of this Agreement.

18. **non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years Company shall not solicit or attempt to solicit Department’s employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to Department with any employee and/or consultant of the Department who has knowledge of the Confidential Information, without the prior written consent of Department. This section will survive irrespective of the fact whether there exists a commercial relationship between Company and Department.

19. Term. Subject to aforesaid section 17, this Agreement shall remain valid up to …. Years from the “effective date”.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For Department	**For Company**
Name:	Name:
Title:	Title:
WITNESSES:	WITNESSES:
1.	1.
2.	2.

SPECIAL CONDITION OF CONTRACT (S.C.C.)

Reference Number	**Amendments of, and Supplements to, Clauses in the General Conditions of Contract**
1.1 (i)	The Client is Bangalore Metropolitan Transport Corporation (BMTC), **BMTC Central Office, Kengal Hanumanthaiah Road, Shanthinagar, Bangalore 560027** The Managed Service Provider is .....

APPENDICES

APPENDIX – A: DESCRIPTION OF THE SERVICES

Refer to Terms of Reference – Section 5

APPENDIX – B: REPORTING REQUIREMENTS

(To be decided at the time of contract signing)

APPENDIX – C: KEY PERSONNEL AND SUB-SERVICE PROVIDER

To be provided by the Service Provider. Refer to Terms of Reference – Section 5

APPENDIX – D: FACILITIES AND SERVICES TO BE PROVIDED BY THE CLIENT

Refer to Terms of Reference – Section 5

APPENDIX – E: BREAKDOWN OF CONTRACT PRICE

As per format in e-procurement portal or format requested by the client in the financial proposal forms- Section 4